世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 G11B 20/10, H04N 5/91	A1	(11) 国際公開番号	WO99/38164
		(43) 国際公開日	1999年7月29日(29.07.99)

(21) 国際出願番号 PCT/JP99/00292

(22) 国際出願日 1999年1月25日(25.01.99)

(30) 優先権データ

特願平10/12474	1998年1月26日(26.01.98)	JP
特願平10/27572	1998年2月9日(09.02.98)	JP

(71) 出願人（米国を除くすべての指定国について）
松下電器産業株式会社
(MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.)[JP/JP]
〒571-8501 大阪府門真市大字門真1006番地 Osaka, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
山田正純(YAMADA, Masazumi)[JP/JP]
〒570-0011 大阪府守口市金田町6-24-10 Osaka, (JP)
飯塚裕之(IITSUKA, Hiroyuki)[JP/JP]
〒576-0033 大阪府交野市私市6-25-6 Osaka, (JP)
後藤昌一(GOTO, Shoichi)[JP/JP]
〒576-0021 大阪府交野市妙見坂5-4-204 Osaka, (JP)
武知秀明(TAKECHI, Hidcaki)[JP/JP]
〒533-0004 大阪府大阪市東淀川区小松4丁目11-10 201号
Osaka, (JP)

(74) 代理人
弁理士 松田正道(MATSUDA, Masamichi)
〒532-0003 大阪府大阪市淀川区宮原5丁目1番3号
新大阪生島ビル Osaka, (JP)

(81) 指定国 CN, KR, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)

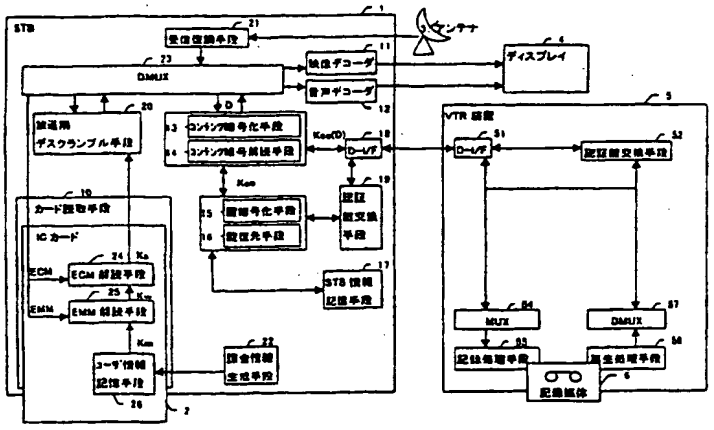
添付公開書類
国際調査報告書

(54)Title: METHOD AND SYSTEM FOR DATA RECORDING / REPRODUCING, APPARATUS FOR RECORDING/REPRODUCING, AND MEDIA FOR RECORDING PROGRAM

(54)発明の名称 データ記録再生方法、データ記録再生システム、記録装置、再生装置、プログラム記録媒体

(57) Abstract

Digital data subjected to first encryption with a content key are recorded together with the content key subjected to second encryption. When the encrypted digital data and the encrypted content key are reproduced, the encrypted content key is decrypted and the decrypted content key is used to recover the digital data.



2 ... IC CARD
3 ... ANTENNA
4 ... DISPLAY
5 ... VTR UNIT
6 ... RECORDING MEDIUM
10 ... CARD READER MEANS
11 ... VIDEO DECODER MEANS
12 ... SOUND DECODER MEANS
13 ... CONTENTS ENCODER MEANS
14 ... CONTENTS DECODER MEANS
15 ... KEY ENCODER MEANS
16 ... KEY DECODER MEANS
17 ... STB INFORMATION STORAGE MEANS
19 ... VERIFICATION KEY EXCHANGE MEANS
20 ... BROADCAST SCRAMBLER MEANS
21 ... RECEIVER-DEMODULATOR MEANS
22 ... CHARGE INFORMATION GENERATOR MEANS
24 ... ECM DECODER MEANS
25 ... EMM DECODER MEANS
26 ... USER INFORMATION STORAGE MEANS
52 ... VERIFICATION KEY EXCHANGE MEANS
55 ... RECORDING PROCESSING MEANS
58 ... REPRODUCTION PROCESSING MEANS

(57)要約

ディジタルデータにコンテンツ鍵を用いて第１の暗号化を施した暗号化ディジタルデータと、前記コンテンツ鍵に第２の暗号化を施した暗号化コンテンツ鍵とを記録媒体に記録し、記録された前記暗号化ディジタルデータおよび前記暗号化コンテンツ鍵を再生し、前記暗号化コンテンツ鍵を解読して得られた前記コンテンツ鍵を用いて前記暗号化ディジタルデータを解読して、前記ディジタルデータを得ることを特徴とするデータ記録再生方法。

明　細　書

データ記録再生方法、データ記録再生システム、記録装置、再生装置、プログラム記録媒体

技術分野

本発明は、著作権等により再生についての期間や回数が制限された、ディジタルデータを記録するデータ記録装置と、そのディジタルデータを再生するデータ再生装置、データ記録再生システムおよびデータ記録再生方法に関するものである。

背景技術

現在、著作権保護の対象となっている映画や音楽等のＡＶデータは、ビデオテープ等に格納されている。ユーザは、そのようなビデオテープ等を有料で貸し出すレンタル店を通じて、例えば１週間というような所定の期間のみビデオテープ等を借り、それを再生することによって、映画や音楽等を鑑賞することができる。

他方、上述したビデオテープ等のレンタルのシステムとは別に、ディジタル技術や暗号化技術の進歩等から、放送局からの映画や音楽等の番組を通信衛星を介して入力し、その番組をコンテンツ暗号化してビデオテープ等に記録し、再生する装置が考えられる。

衛星放送の録画、再生をユーザーが自由に行えると、少数のユーザーを介して、不特定多数の者に、録画された番組が無制限に供給されることが可能

になるため、この対策を講ずることは、プロバイダにとって必要不可欠なことである。まず、希望の番組を視聴する場合の手順について説明する。ユーザーが視聴希望の番組を選択すると、その番組の視聴料金に対応する視聴用課金情報が、ＩＣカードに記録される。原則として各番組のデータには、スクランブルがかけられており、当該番組の視聴用課金情報が、ＩＣカードに記録されている場合のみ、ＳＴＢがスクランブルを解除して、スクランブルがない状態でディスプレイが映像出力する。ただし、ＳＴＢがスクランブルを解除しても、当該ＡＶデータにはコピー防止信号（マクロビジョン）がかかっているため、この状態で、記録媒体に記録しても、再生時の再生画像が乱れてしまう。

次に、希望の番組を録画／再生する場合の手順について説明する。ユーザーが録画希望の番組を選択すると、その番組の録画料金に対応する録画用課金情報が、ＩＣカードに記録される。当該番組の録画用課金情報が、ＩＣカードに記録されている場合のみ、ＳＴＢが前述したマクロビジョンを解除して、乱れのないＡＶデータをＶＴＲ装置に出力し、ＶＴＲ装置は、これを記録媒体に記録する。記録されたＡＶデータは、マクロビジョンがかかってないため、通常のＡＶデータと同様の再生方法で、映像出力が得られる。

以上の手順で、ＩＣカードに記録された視聴用課金情報および録画用課金情報は、一定期間分が電話回線等によって、プロバイダに通知される。

ＳＴＢ装置とＶＴＲ装置が分離したタイプの衛星放送のデータ記録再生システムについて説明したが、各装置の機能を一つの装置に集約したタイプのものもある。

ところで、上述したビデオテープ等のレンタルのシステムは、これからの

多チャンネルディジタル放送時代においても、ユーザがその都度レンタル店に出向いてビデオテープ等を借りなければならないという点など、ユーザにとって相変わらず手間がかかり不便である。

しかしながら、上述した記録再生方法では、一度記録された記録媒体は、何回でも再生でき、また、当該記録媒体を複製することも容易に行えるという問題点がある。

従来の記録再生装置では、映画や音楽等の著作権保護の対象となっているＡＶデータの有効再生期間や有効再生回数には制限がないということになる。例えば、劇場放映直後の映画のように、特別な価値を有するＡＶデータが上述したような、再生の期間や回数について制限のない記録再生装置によって記録媒体に記録されると、そのＡＶデータの価値は半減する。つまり、放送局は、そのような特別な価値を有するＡＶデータを安心して放送することができない。

上記問題点の対策として、ＡＶデータが記録された記録媒体に、当該ＡＶデータ記録時に使用したＳＴＢおよび／またはＶＴＲ装置のＩＤも記録しておき、ＩＤが異なる機器で再生しようとすると、再生できないようにするという方法が提案されている。しかし、ＩＤ識別機能を有しない機器を用いる場合は、ＩＤの一致に関わりなく再生が可能であるという課題がある。また、全ての機器がＩＤ識別機能を有するとの前提に立てば、機器固有のＩＤを用いているために、当該機器が修復不可能な故障・破損等によって、使用できなくなった場合には、当該記録媒体に記録されたＡＶデータは、再生が不可能になってしまうという課題がある。

発明の開示

本発明は、上述した従来のデータ記録再生方法の課題を考慮し、データに暗号化を施すことによって、特定の対象に対してのみ、再生が可能であり、前記暗号化に関する情報が外部に漏洩しにくいデータ記録再生方法およびデータ記録再生システムを提供することを第一の目的とするものである。

また、前記第一の目的に加え、記録および／または再生時に、確実に課金が可能なデータ記録再生方法およびデータ記録再生システムを提供することを目的とするものである。

さらに、前記第一の目的に加え、再生時のロスタイムが少ないデータ記録再生システムを提供することを目的とするものである。

また、本発明は、データを記録媒体に記録し、そのデータの有効再生期間や有効再生回数の制限を遵守する記録装置および再生装置を提供することを目的とするものである。

図面の簡単な説明

図１は、本発明の第１の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

図２は、本発明の第１の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図３は、本発明の第１の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図４は、本発明の第１の実施の形態におけるデータ記録再生システムを用いて記録された記録媒体上の記録領域を示す模式図である。

図５は、本発明の第２の実施の形態におけるデータ記録再生システムで記録された記録媒体の貸与時の流れを示すフロー図である。

図６は、本発明の第３の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図７は、本発明の第３の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図８は、本発明の第４の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図９は、本発明の第４の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図１０は、本発明の第５の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

図１１は、本発明の第５の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図１２は、本発明の第５の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図１３は、本発明の第５の実施の形態における別のデータ記録再生システムの構成を示す構成図である。

図１４は、本発明の第５の実施の形態における別のデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図１５は、本発明の第６の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

図１６は、本発明の第６の実施の形態におけるデータ記録再生システムの

データ記録時のデータの流れを示すフロー図である。

図１７は、本発明の第６の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図１８は、本発明の第６の実施の形態における別のデータ記録再生システムの構成を示す構成図である。

図１９は、本発明の第６の実施の形態における別のデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図２０は、本発明の第６の実施の形態における別のデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図２１は、本発明の第７の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図２２は、本発明の第７の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図２３は、本発明の第８の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

図２４は、本発明の第８の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図２５は、本発明の第８の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図２６は、本発明の第９の実施の形態の記録装置および再生装置のブロック図である。

図２７は、本発明の第９の実施の形態の記録装置および再生装置に使用される鍵暗号化鍵Ｋｘリストの一例を示す図である。

図２８は、図２６とは異なる本発明の記録装置および再生装置のブロック図である。

図２９は、図２６または２８とは異なる本発明の記録装置および再生装置のブロック図である。

図３０は、図２６、２８または２９とは異なる本発明の記録装置および再生装置のブロック図である。

図３１は、図２６、２８、２９または３０とは異なる本発明の記録装置および再生装置のブロック図である。

発明を実施するための最良の形態

以下に、本発明の実施の形態を図面を参照して説明する。

（第１の実施の形態）

以下に、本発明の第１の実施の形態を図面を参照して説明する。

図１は、本発明の第１の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムは、本発明のチューナ装置に対応するＳＴＢ（Ｓｅｔ　Ｔｏｐ　Ｂｏｘ；衛星放送受信機）１と、ＳＴＢ１にユーザーＩＤ等の情報を与えるＩＣカード２と、ＳＴＢ１に接続されているアンテナ３およびディスプレイ４と、本発明のＶＴＲ装置に対応するＶＴＲ装置５と、ＶＴＲ装置５によってデータを記録／再生される記録媒体６とから構成されている。

ＳＴＢ１は、ＩＣカード２に記録された情報の読み取り、必要情報をＩＣカード２に記録するカード読取手段１０と、ＳＴＢ１の機器ＩＤ等の情報を

記憶するＳＴＢ情報記憶手段１７と、ディスプレイ４に対してデコードされたＡＶデータを出力する映像デコーダ１１および音声デコーダ１２と、コンテンツ鍵を生成し、ＡＶデータに前記コンテンツ鍵を用いて暗号化を施して暗号化ＡＶデータを生成するコンテンツ暗号化手段１３と、前記コンテンツ鍵に第２の暗号化を施して暗号化コンテンツ鍵を生成する鍵暗号化手段１５と、前記暗号化コンテンツ鍵を解読して前記コンテンツ鍵を復元する鍵暗号解読手段１６と、復元された前記コンテンツ鍵を用いて前記暗号化ＡＶデータを解読して、前記ＡＶデータを得るコンテンツ暗号解読手段１４と、ＶＴＲ装置５と直接データの伝達を行うＤ－Ｉ／Ｆ（ディジタルインターフェイス）１８およびＶＴＲ装置５と認証鍵の交換を行ってＶＴＲ装置５の確認を行う認証鍵交換手段１９と、人工衛星からの電波をアンテナ３を介して受信して、受信したデータの復調を行いＳＴＢ１内部用の信号に変換する受信復調手段２１と、受信したデータに施されている放送用暗号を解除する放送用デスクランブル手段２０と、多重化されている受信データを分離するＤＭＵＸ（Ｄｅ－ｍｕｌｔｉｐｌｅｘｅｒ；分離部）２３とを有している。なお、ＳＴＢ１は、上記の他に、ＳＴＢ１の装置全体を制御するＳＴＢ制御手段（図示せず）を備えている。

ＶＴＲ装置５は、ＳＴＢ１と直接データの伝達を行うＤ－Ｉ／Ｆ（ディジタルインターフェイス）５１およびＳＴＢ１と認証鍵の交換を行ってＳＴＢ１の確認を行う認証鍵交換手段５２と、前記暗号化ＡＶデータおよび前記暗号化コンテンツ鍵に対して記録媒体６のフォーマットに適合した多重化を行うＭＵＸ（Ｍｕｌｔｉｐｌｅｘｅｒ；多重化部）５４および多重化されたデータを記録媒体６に記録する記録処理手段５５と、記録媒体６に記録された

データを再生する再生処理手段５８および多重化された再生データを分離するＤＭＵＸ（Ｄｅ－ｍｕｌｔｉｐｌｅｘｅｒ；分離部）５７とを備えている。なお、ＶＴＲ装置５は、上記の他に、ＶＴＲ装置５の装置全体を制御するＶＴＲ制御手段（図示せず）を備えている。

次に、このような本実施の形態の動作を説明する。

まず、ＡＶデータを記録媒体６に記録する時のデータの流れを図２を用いて説明する。図２は、本発明の第１の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。図２において、図１で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、Ｄは、記録しようとするＡＶデータの生（Plain）データを、Ｋｃｏは、ＡＶデータＤの暗号化に用いるコンテンツ鍵を、Ｋｃｏ（Ｄ）は、ＡＶデータＤにコンテンツ鍵Ｋｃｏを用いて暗号化を施して得られる暗号化ＡＶデータを、 STBＰａは、コンテンツ鍵Ｋｃｏの暗号化に用いるＳＴＢ１に固有の公開鍵を、 STBＰａ（Ｋｃｏ）は、コンテンツ鍵Ｋｃｏに公開鍵 STBＰａを用いて暗号化を施して得られる暗号化コンテンツ鍵を、それぞれ示す。なお、本実施の形態におけるデータ記録再生システムは、コンテンツ鍵Ｋｃｏを、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

先ず、受信復調手段２１は、アンテナ３を介して受信した、放送局からの、ディジタルの映像データ、音声データ、ＥＭＭ（個別情報）、ＥＣＭ（番組情報）および暗号化された放送スクランブル鍵Ｋｓを入力し、映像データおよび音声データの信号波形の乱れを整形し、映像データ、音声データ、Ｅ

MM、ＥＣＭおよび暗号化された放送スクランブル鍵Ｋｓを DMUX２３に出力する。

ＥＭＭ（個別情報）は、後に説明するワーク鍵Ｋｗという鍵を生成するさいに必要となる情報である。

さらに、ＥＣＭ（番組情報）は、暗号化された放送スクランブル鍵Ｋｓを復元するさいに必要となる情報である。

その後、DMUX２３は、受信復調手段２１からの映像データ、音声データ、EMM、ＥＣＭおよび放送スクランブル鍵Ｋｓを入力して分離し、映像データおよび音声データ（ＡＶデータ）を放送デスクランブル手段２０に出力する。また、ＥＭＭをＥＭＭ解読手段２５に出力し、ＥＣＭおよび暗号化された放送スクランブル鍵ＫｓをＥＣＭ解読手段２４に出力する。

次に、ＥＭＭ解読手段２５は、ユーザＩＤ鍵Ｋｍを入力するとともに、DMUX２３からのＥＭＭを入力し、ユーザＩＤ鍵ＫｍでＥＭＭを解読してワーク鍵Ｋｗを生成し、ＥＣＭ解読手段２４に出力する。

さらに、ＥＣＭ解読手段２４は、ＥＭＭ解読手段２５からのワーク鍵Ｋｗを入力するとともに、DMUX２３からの、ＥＣＭおよび暗号化された放送スクランブル鍵Ｋｓを入力し、ワーク鍵ＫｗでＥＣＭを解読して、暗号化された放送スクランブル鍵Ｋｓの暗号化を復元し、放送デスクランブル手段２０に出力する。

そして、放送デスクランブル手段２０は、ＥＣＭ解読手段２４からの放送スクランブル鍵Ｋｓを入力するとともに、DMUX２３からの、スクランブルされたＡＶデータを入力し、放送スクランブル鍵Ｋｓで、スクランブルされたＡＶデータをデスクランブルする。

ＡＶデータＤは、放送用のスクランブルを放送用デスクランブル手段２０で解除され、ＤＭＵＸ２３で分離されて、生のＡＶデータＤとなって、映像デコーダ１１および音声デコーダ１２およびコンテンツ暗号化手段１３へ送られる。映像デコーダ１１および音声デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、ディスプレイ４へ出力する。

コンテンツ暗号化手段１３は、コンテンツ鍵Ｋｃｏを生成し、生成したコンテンツ鍵Ｋｃｏを用いて、ＡＶデータＤに暗号化を施して、暗号化ＡＶデータＫｃｏ（Ｄ）を生成する。生成されたコンテンツ鍵Ｋｃｏは、鍵暗号化手段１５へ送られ、鍵暗号化手段１５は、ＳＴＢ情報記憶手段１７に記憶されているＳＴＢ１に固有の公開鍵 STBPａを用いて、コンテンツ鍵Ｋｃｏに暗号化を施して、暗号化コンテンツ鍵 STBPａ（Ｋｃｏ）を生成する。

暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、暗号化コンテンツ鍵 STBPａ（Ｋｃｏ）は、認証鍵交換手段１９およびＤ－Ｉ／Ｆ１８を介して、それぞれＶＴＲ装置５へ伝達されるが、それに先だって、ＳＴＢ１、ＶＴＲ装置５それぞれの認証鍵交換手段１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

ＶＴＲ装置５へ伝達された暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、暗号化コンテンツ鍵 STBPａ（Ｋｃｏ）は、Ｄ－Ｉ／Ｆ５１および認証鍵交

換部５２を介して、それぞれＭＵＸ５４へ送られて、記録媒体６のフォーマットに適合した多重化を行われた後、記録処理手段５５によって、記録媒体６に記録される。

次に、記録媒体６に記録されたＡＶデータを再生する時のデータの流れを図３を用いて説明する。図３は、本発明の第１の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図３において、図１で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。 STBＳａは、公開鍵 STBＰａに対応し、暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ）を解読してコンテンツ鍵Ｋｃｏを復元するのに用いるＳＴＢ１に固有の秘密鍵を示す。図中の他の記号は、図２に倣う。

多重化されて記録媒体６に記録された暗号化ＡＶデータＫｃｏ（Ｄ）および暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ）は、再生処理手段５８により再生され、ＤＭＵＸ５７で分離される。

分離された暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、分離された暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ）は、認証鍵交換手段５２およびＤ－Ｉ／Ｆ５１を介して、それぞれＳＴＢ１へ伝達されるが、それに先だって、記録時と同様に、ＳＴＢ１、ＶＴＲ装置５それぞれの認証鍵交換手段１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

ＳＴＢ１へ伝達された暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、コンテンツ暗号解読手段１４へ送られ、暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ）は、Ｄ－Ｉ／Ｆ１８および認証鍵交換手段１９を介して、鍵暗号解読手段１６へ送られる。鍵暗号解読手段１６は、ＳＴＢ情報記憶手段１７に記憶されているＳＴＢ１に固有の秘密鍵STBＳａを用いて、暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ）をコンテンツ鍵Ｋｃｏに復元して、コンテンツ暗号解読手段１４へ送る。コンテンツ暗号解読手段１４は、復元されたコン

テンツ鍵Ｋｃｏを用いて、暗号化ＡＶデータＫｃｏ（Ｄ）を解読して得られるＡＶデータＤを、映像デコーダ１１および音声デコーダ１２へ出力する。映像デコーダ１１および音声デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、ディスプレイ４へ出力する。

以上の手順にしたがって、ＡＶデータを記録／再生することにより、ＡＶデータに暗号化を施すのに用いたコンテンツ鍵にＳＴＢ１に固有の公開鍵を用いて暗号化を施して、暗号化されたＡＶデータと一緒に記録媒体に記録し、再生時には暗号化されたコンテンツ鍵をＳＴＢ１に固有の秘密鍵を用いて復元しているため、ＳＴＢ１に固有の秘密鍵を持っているシステム、すなわち、ＳＴＢ１そのものを備えているシステムしか再生できないので、本実施の形態におけるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであることがわかる。

次に、本実施の形態におけるデータ記録再生システムの課金方法について説明する。本課金方法は、ＡＶデータの記録／再生時に課金するものであるため、図２、図３を参照して説明する。

まず、記録時の課金方法について説明する。図２において、ＳＴＢ１のＳＴＢ制御手段（図示せず）は、記録時に、課金情報生成手段２２を用いて課金情報を生成し、これをカード読取手段１０を介して、ＩＣカード２に記録させる。記録のタイミングとしては、例えば、ユーザーからの記録指令に連動して記録するとしてもよいし、コンテンツ暗号化手段１３または鍵暗号化手段１５の最初の出力に連動して記録するとしてもよい。記録する課金情報の内容としては、課金の金額そのものを記録するものであってもよいし、課

金内容を特定するための識別子のようなものであってもよい。

次に、再生時の課金方法について説明する。図３において、ＳＴＢ１のＳＴＢ制御手段（図示せず）は、再生時に、課金情報生成手段２２を用いて課金情報を生成し、これをカード読取手段１０を介して、ＩＣカード２に記録する。記録のタイミングとしては、例えば、ユーザーからの再生指令に連動して記録するとしてもよいし、コンテンツ暗号解読手段１４または鍵暗号解読手段１６の最初の出力に連動して記録するとしてもよい。記録する課金情報の内容については、記録時と同様である。

ＩＣカード２に記録された課金情報は、定期的または不定期に、衛星放送のサービスプロバイダに対して、電話回線等の通信を介して出力され、サービスプロバイダは、この課金情報に基づいて、ユーザーの銀行口座からの引き落とし等の方法によって、ユーザーから課金の徴収を行う。

なお、上記説明において、課金情報は記録時および再生時に記録する、すなわち、記録、再生の両方に対して課金を行うとして説明したが、これに限らず、いずれか一方についてのみ、課金を行うとしてもよい。

また、課金情報は、カード読取手段１０を介して、ＩＣカード２に記録されるとして説明したが、これに限らず、例えば、ＳＴＢ情報記憶手段１７に記録されるとしてもよい。なお、ＳＴＢ情報記憶手段１７に記録される場合は、本実施の形態の構成におけるデータ記録再生システムから、ＩＣカード２およびカード読取手段１０を省いてもよい。

また、再生時の課金情報は、再生期間の限定および／または再生回数の限定を伴っていてもよい。例えば、ある期間を過ぎる、またはある再生回数を超えると、課金の金額が変わるというものでもよい。ただし、再生回数の限

定を伴う場合には、再生する毎に、記録媒体６等に通算再生回数を示す情報を書き込む必要がある。

さらに、記録時に、再生時の課金情報を生成するために必要な情報を、記録媒体６に記録し、記録媒体６の再生時に前記必要な情報を用いて課金情報を生成するとしてもよい。このときは、例えば、ＳＴＢ制御手段が記録時に前記必要な情報を生成し、これを、Ｄ－Ｉ／Ｆ１８および５１を介して、記録処理手段５５に送り、記録処理手段５５は、記録データの最初にこれを記録する。再生時には、前記必要な情報は、再生処理手段５８によって再生され、Ｄ－Ｉ／Ｆ１８および５１を介して、ＳＴＢ制御手段へ送られ、ＳＴＢ制御手段は、これに基づいて、課金情報生成手段２２を用いて再生時の課金情報を生成する。

以上説明したところから、本実施の形態におけるデータ記録再生システムは、記録および／または再生時に、確実に課金が可能なデータ記録再生システムであることがわかる。

次に、本実施の形態におけるデータ記録再生システムによって、記録媒体に記録されるデータの、記録媒体上の記録領域について、図２、図４を参照して説明する。

図４は、本発明の第１の実施の形態におけるデータ記録再生システムを用いて記録された記録媒体上の記録領域を示す模式図である。図４の左右方向は、記録媒体６の時間的な記録位置を示し、上下方向は、同時刻に記録されたデータの構成を示す。図４において、記録領域は、メインエリアとサブエリアとに分けられており、メインエリアには、暗号化ＡＶデータと、コンテンツ鍵変更のタイミングを示すフラッグとが書き込まれており、サブエリア

には、当該記録位置に対応するメインエリアの位置に記録された暗号化ＡＶデータ（Ｋｃｏ－ａ（Ｄ）、Ｋｃｏ－ｂ（Ｄ）、Ｋｃｏ－ｃ（Ｄ）、Ｋｃｏ－ｄ（Ｄ）、．．．）の暗号化に用いられたコンテンツ鍵（Ｋｃｏ－ａ、Ｋｃｏ－ｂ、Ｋｃｏ－ｃ、Ｋｃｏ－ｄ、．．．）に、公開鍵 STBＰａを用いて暗号化を施して得られた、暗号化コンテンツ鍵（ STBＰａ（Ｋｃｏ－ａ）、STBＰａ（Ｋｃｏ－ｂ）、STBＰａ（Ｋｃｏ－ｃ）、STBＰａ（Ｋｃｏ－ｄ）、．．．）と、次のコンテンツ鍵の切替後に用いられるコンテンツ鍵（Ｋｃｏ－ｂ、Ｋｃｏ－ｃ、Ｋｃｏ－ｄ、Ｋｃｏ－ｅ、．．．）に、公開鍵 STBＰａを用いて暗号化を施して得られた、暗号化コンテンツ鍵（ STBＰａ（Ｋｃｏ－ｂ）、STBＰａ（Ｋｃｏ－ｃ）、STBＰａ（Ｋｃｏ－ｄ）、STBＰａ（Ｋｃｏ－ｅ）、．．．）とが書き込まれている。ただし、図４中においては、暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ－ａ）、STBＰａ（Ｋｃｏ－ｂ）、STBＰａ（Ｋｃｏ－ｃ）、STBＰａ（Ｋｃｏ－ｄ）、．．．は、便宜上、暗号化前のコンテンツ鍵Ｋｃｏ－ａ、Ｋｃｏ－ｂ、Ｋｃｏ－ｃ、Ｋｃｏ－ｄ、．．．で表現している。

前述したように、コンテンツ暗号化手段１３は、コンテンツ鍵Ｋｃｏを定期的または不定期的に切り替えて生成し、生成したコンテンツ鍵Ｋｃｏを用いて、ＡＶデータＤに暗号化を施して、暗号化ＡＶデータＫｃｏ（Ｄ）を生成するが、現在使用中のコンテンツ鍵（例えば、Ｋｃｏ－ａ）の次の切替後のコンテンツ鍵（例えば、Ｋｃｏ－ｂ）をあらかじめ生成して、その使用に先立って、鍵暗号化手段１５により暗号化コンテンツ鍵STBＰａ（Ｋｃｏ－ａ）に変換して、認証鍵交換手段１９、Ｄ－Ｉ／Ｆ１８、５１を介して、ＭＵＸ５４へ送り、記録処理手段５５は、これを現在使用中のコンテンツ鍵Ｋｃ

ｏ－ａ、それによって暗号化された暗号化ＡＶデータＫｃｏ－ａ（Ｄ）等とともに、図４に示した記録領域に記録する。なお、コンテンツ鍵変更のタイミングを示すフラッグは、例えば、ＡＶデータを伝送するパケットヘッダに付加されて伝達されてくるものとし、記録処理手段５５は、これをもとに、各記録データの記録位置を決定する。

図４に示すように、切り替えの後のコンテンツ鍵、例えば、Ｋｃｏ－ｂ、に対応する暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ－ｂ）は、切り替えの前のコンテンツ鍵Ｋｃｏ－ａに対応する暗号化ＡＶデータＫｃｏ－ａ（Ｄ）の少なくとも一部と重なるように、記録媒体６に記録されており、切り替えの前のコンテンツ鍵Ｋｃｏ－ａは、それに対応する暗号化ＡＶデータＫｃｏ－ａ（Ｄ）が記録されている位置に重なって、記録媒体６に記録されている。なお、暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ－ｂ）の記録領域は、図４においては、その次のコンテンツ鍵Ｋｃｏ－ｃに対応する暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ－ｃ）が書き込まれる直前まで書き込まれているが、少なくとも暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ－ｃ）が書き込まれる前に書き込みが終了していればよい、すなわち、図４中の暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ－ｂ）の記録領域は、少なくとも暗号化ＡＶデータＫｃｏ－ａ（Ｄ）の一部と重なるように記録されておれば、暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ－ｃ）の記録領域の始端との間にデータの空白領域があってもよい。

以上の記録要領によって、記録媒体への記録を行うことによって、再生時には、次のコンテンツ鍵をあらかじめ解読できるので、本実施の形態におけるデータ記録再生システムは、再生時のロスタイムが少ないデータ記録再生システムであることがわかる。

なお、本発明の記録媒体上の記録領域への記録要領は、本実施の形態における上述した記録要領に限るものではなく、例えば、コンテンツ暗号化手段１３が次の切替後のコンテンツ鍵をあらかじめ生成せず、ＶＴＲ装置５が、ＳＴＢ１から送られてくるデータを一時記憶する手段を有し、前記一時記憶する手段に現在のデータを一時記憶させて、コンテンツ鍵切替後のデータを受け取った後に、記録媒体６への記録領域を決定して、記録するとしてもよい。

また、上述した記録要領に加えて、コンテンツ鍵Ｋｃｏの暗号化に用いた鍵を特定できる情報を記録媒体６に記録するとしてもよい。具体的には、本実施の形態においては、ＳＴＢ１のＩＤ情報である。この情報を利用して、例えば、ＳＴＢ１以外のＳＴＢを用いて再生をしようとした場合、当該ＳＴＢでは再生できない旨の警告とともに、再生可能なＳＴＢ（ここではＳＴＢ１）のＩＤ情報を表示することができる。

また、暗号化コンテンツ鍵を記録媒体６中の外部に出力されないデータ領域に記録してもよい。例えば、Ｄ－ＶＨＳシステムであれば、サブコード領域に記録する。これによって、さらに、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムとなる。

さらに、本実施の形態においては、暗号化ディジタルデータおよび暗号化コンテンツ鍵は、記録媒体上の再生のタイミングに対応する記録位置に記録されるとして説明したが、これに限るものではなく、記録位置にとらわれず、切り替えの後のコンテンツ鍵に対応する暗号化コンテンツ鍵が、切り替えの前のコンテンツ鍵に対応する暗号化ディジタルデータの少なくとも一部とタイミング的に重なるように、また、一つのコンテンツ鍵に対応する暗号化

コンテンツ鍵が、それに対応する暗号化ディジタルデータとタイミング的に重なるように、再生されさえすればよい。

なお、上述した本実施の形態の課金方法および／または記録媒体上の記録領域への記録要領の替わりに、従来のものを用いる場合においては、上述したそれぞれの効果は得られないものの、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生方法およびデータ記録再生システムを提供するという、本発明の第一の目的は満足するものである。

（第２の実施の形態）

以下に、本発明の第２の実施の形態を図面を参照して説明する。本実施の形態が上述した第１の実施の形態と異なる点は、コンテンツ鍵の暗号化／復元を行う公開鍵／秘密鍵が、本発明のチューナ装置の機器モデルに対して固有な鍵であることに関する点である。したがって、本実施の形態において、第１の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第１の実施の形態と同じとする。

本実施の形態におけるデータ記録再生システムの構成は、第１の実施の形態におけるデータ記録再生システムの構成と同じである。

次に、このような本実施の形態の動作を説明する。

本実施の形態においては、コンテンツ鍵Ｋｃｏの暗号化にＳＴＢ１の機器モデルに固有の公開鍵STBUＰａを用い、コンテンツ鍵Ｋｃｏを復元するのにＳＴＢ１の機器モデルに固有の秘密鍵STBUＳａを用いている点以外は、第１の実施の形態におけるデータ記録再生システムと同じである。したがって、本実施の形態の動作は、図２、図３において、公開鍵 STBＰａ、秘密鍵 STB

Ｓａおよび暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ）を、それぞれ、公開鍵STBUＰａ、秘密鍵STBUＳａおよび暗号化コンテンツ鍵STBUＰａ（Ｋｃｏ）に置き換えたもので示されるので、詳細の説明は、図２、図３に倣うとして省略する。

以上の手順にしたがって、ＡＶデータを記録／再生することにより、本実施の形態は、第１の実施の形態によって得られる効果に加え、図５に示すように、ＳＴＢ１と同じモデルであるＳＴＢ１０１を所有しているユーザー間での記録媒体６の貸し借りが可能となり、かつ、ＳＴＢ１が修復不可能な故障・破損等によって、使用できなくなった場合においても、同じ機器モデルのＳＴＢに代替すれば、引き続き使用できるものであることがわかる。

（第３の実施の形態）

以下に、本発明の第３の実施の形態を図面を参照して説明する。本実施の形態が上述した第１の実施の形態と異なる点は、コンテンツ鍵の暗号化／復元を行う公開鍵／秘密鍵が、本発明のＩＣカードに記録されたユーザＩＤに対して固有な鍵であることに関する点である。したがって、本実施の形態において、第１の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第１の実施の形態と同じとする。

本実施の形態におけるデータ記録再生システムの構成は、第１の実施の形態におけるデータ記録再生システムの構成と同じである。

次に、このような本実施の形態の動作を説明する。

図６は、本発明の第２の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図であり、図７は、本発明の第２の

実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図６、図７に示すとおり、本実施の形態においては、コンテンツ鍵Ｋｃｏの暗号化にＩＣカード２に記録されたユーザＩＤに対して固有の公開鍵USERＰａを用い、コンテンツ鍵Ｋｃｏを復元するのにユーザＩＤに対して固有の秘密鍵USERＳａを用いている点以外は、第１の実施の形態におけるデータ記録再生システムと同じである。

以上の手順にしたがって、ＡＶデータを記録／再生することにより、本実施の形態は、第１の実施の形態によって得られる効果に加え、ＳＴＢ１が修復不可能な故障・破損等によって、使用できなくなった場合においても、他のＳＴＢ（同じ機器モデルでなくても可）に代替すれば、引き続き使用でき、かつ、ＩＣカード２と一緒に記録媒体６の貸し借りをすれば、他のユーザーの使用が可能となるものであることがわかる。

また、本実施の形態において、上述のようにコンテンツ鍵Ｋｃｏの暗号化にＩＣカード２に記録されたユーザＩＤに対して固有の公開鍵USERＰａを用いて、暗号化コンテンツ鍵USERＰａ（Ｋｃｏ）を生成するとともに、同じくＩＣカード２に記録された他のユーザＩＤに対して固有の公開鍵 USER1Ｐａを用いて、暗号化コンテンツ鍵 USER1Ｐａ（Ｋｃｏ）も生成して、暗号化コンテンツ鍵USERＰａ（Ｋｃｏ）とともに、記録媒体６に記録しておけば、ＩＣカード２を貸し出さなくても、公開鍵 USER1Ｐａに対応する秘密鍵 USER1Ｓａを保持している特定のユーザーは、その USER1Ｓａを用いて暗号化コンテンツ鍵 USER1Ｐａ（Ｋｃｏ）を復元できるので、その特定のユーザーに対してのみ、記録媒体６の貸し出し使用が可能となる。なお、公開鍵 USER1Ｐａは、単数に限るものではなく、公開鍵 USER1Ｐａ～ USERnＰａと、複数個

であってもよい。すなわち、ユーザーは、貸し出し使用をしたい他のユーザーが生じた場合には、所定の手続を経て、ＩＣカード２に、当該他のユーザーに対応する公開鍵 USERnＰａを記録して貰うことによって、当該他のユーザーへの簡単な貸し出し使用が可能となるものである。

なお、上記動作からわかるように、本実施の形態においては、図１に示した第１の実施の形態におけるデータ記録再生システムの構成から、ＳＴＢ記憶手段１１を省略したものであってもよい。

（第４の実施の形態）

以下に、本発明の第４の実施の形態を図面を参照して説明する。本実施の形態が上述した第１の実施の形態と異なる点は、コンテンツ鍵の暗号化／復元を行う公開鍵／秘密鍵が、本発明のＩＣカードに記録されたサービスに対して固有な鍵であることに関する点である。したがって、本実施の形態において、第１の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第１の実施の形態と同じとする。

本実施の形態におけるデータ記録再生システムの構成は、第１の実施の形態におけるデータ記録再生システムの構成と同じである。

次に、このような本実施の形態の動作を説明する。

図８は、本発明の第４の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図であり、図９は、本発明の第４の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図８、図９に示すとおり、本実施の形態においては、コンテンツ鍵Ｋｃｏの暗号化にＩＣカード２に記録されたサービスに対し

て固有の公開鍵SERVＰａを用い、コンテンツ鍵Ｋｃｏを復元するのにＳＴＢ１の機器モデルに固有の秘密鍵SERVＳａを用いている点以外は、第１の実施の形態におけるデータ記録再生システムと同じである。ここで、サービスに対して固有の鍵とは、具体的には、特定の番組に対してのみ固有、特定のジャンルの番組に対してのみ固有、特定のチャンネル番組に対してのみ固有、特定の衛星放送のプロバイダに対してのみ固有の鍵等が挙げられる。

例えば、特定の番組の記録／再生に対して、前もって料金を支払うことにより、その番組に固有の公開鍵SERVＰａおよび秘密鍵SERVＳａをＩＣカード２に記憶させてもらうことにより、前記特定の番組の記録／再生が可能となるものである。この場合、公開鍵SERVＰａおよび秘密鍵SERVＳａがＩＣカード２に記憶されていなければ、記録できなくなる措置をＳＴＢ１が有する必要がある。なお、公開鍵SERVＰａおよび秘密鍵SERVＳａが必要な特定の番組以外の番組に対しては、第１～第３の実施の形態のいずれかで用いた公開鍵および秘密鍵に切り替えて、これらを用いるという、併用も可能である。

以上の手順にしたがって、ＡＶデータを記録／再生することにより、本実施の形態は、第１の実施の形態によって得られる効果に加え、ＳＴＢ１が修復不可能な故障・破損等によって、使用できなくなった場合においても、他のＳＴＢ（同じ機器モデルでなくても可）に代替すれば、引き続き使用でき、かつ、記録されたＡＶデータに対応する特定のサービスを享受することを許可された特定のユーザーに対してのみ、記録媒体６の貸し借り使用が可能となるものであることがわかる。

なお、上記動作からわかるように、本実施の形態においては、図１に示した第１の実施の形態におけるデータ記録再生システムの構成から、ＳＴＢ記

憶手段１１を省略したものであってもよい。

（第５の実施の形態）

以下に、本発明の第５の実施の形態を図面を参照して説明する。本実施の形態が上述した第１の実施の形態と異なる点は、本発明の鍵暗号化手段がＶＴＲ装置に備えられており、それに伴って、本発明のチューナ装置が、コンテンツ鍵を共通鍵によって暗号化する第二の鍵暗号化手段を有し、本発明のＶＴＲ装置が、前記共通鍵によって暗号化された前記コンテンツ鍵を解読する第二の鍵暗号解読手段を有することに関する点である。したがって、本実施の形態において、第１の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第１の実施の形態と同じとする。

図１０は、本発明の第５の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムの構成が、第１の実施の形態におけるデータ記録再生システムの構成と異なるのは、本発明の鍵暗号化手段に対応する鍵暗号化手段６２が、ＳＴＢ１ではなく、ＶＴＲ装置５に備えられており、それに伴い、ＳＴＢ１は、本発明の第二の鍵暗号化手段に対応する鍵暗号化手段３１を有し、ＶＴＲ装置５は、本発明の第二の鍵暗号解読手段に対応する鍵暗号解読手段６１と、鍵暗号解読手段６１および鍵暗号化手段６２が用いる共通鍵、公開鍵等の情報を記憶するＶＴＲ情報記憶手段７１とを有している。また、ＳＴＢ情報記憶手段１７は、第１の実施の形態において保持していた情報に加えて、鍵暗号化手段３１がコンテンツ鍵を暗号化するのに用いる共通鍵の情報を保持している。

なお、第１の実施の形態と同様に、課金情報が、例えば、ＳＴＢ情報記憶

手段１７に記録される場合は、本実施の形態の構成におけるデータ記録再生システムから、ＩＣカード２およびカード読取手段１０を省いてもよい。

次に、このような本実施の形態の動作を説明する。

まず、ＡＶデータを記録媒体６に記録する時のデータの流れを図１１を用いて説明する。図１１は、本発明の第５の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。図１１において、図１０で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、図中の記号については、新たに説明するもの以外は、図２、図３に倣う。Ｋｋは、コンテンツ鍵Ｋｃｏの暗号化に用いるＳＴＢ１およびＶＴＲ装置５に共通な共通鍵を、ＡＶデータＤの暗号化に用いるコンテンツ鍵を、Ｋｋ（Ｋｃｏ）は、コンテンツ鍵Ｋｃｏに共通鍵Ｋｋを用いて暗号化を施して得られる暗号化コンテンツ鍵を、それぞれ示す。なお、本実施の形態におけるデータ記録再生システムは、第１の実施の形態と同様に、コンテンツ鍵Ｋｃｏを、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

放送用電波として暗号化され、多重化されたＡＶデータＤは、アンテナ３を介して受信され、受信復調手段２１で復調され、放送用の暗号を放送用デスクランブル手段２０で解除され、ＤＭＵＸ２３で分離されて、生のＡＶデータＤとなって、映像デコーダ１１および音声デコーダ１２およびコンテンツ暗号化手段１３へ送られる。映像デコーダ１１および音声デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、ディスプレイ４へ出力する。コンテンツ暗号化手段１３は、コンテンツ鍵Ｋｃｏを生成し

、生成したコンテンツ鍵Ｋｃｏを用いて、ＡＶデータＤに暗号化を施して、暗号化ＡＶデータＫｃｏ（Ｄ）を生成する。生成されたコンテンツ鍵Ｋｃｏは、鍵暗号化手段３１へ送られ、鍵暗号化手段３１は、ＳＴＢ情報記憶手段１７に記憶されているＳＴＢ１およびＶＴＲ装置５に共通な共通鍵Ｋｋを用いて、コンテンツ鍵Ｋｃｏに暗号化を施して、暗号化コンテンツ鍵Ｋｋ（Ｋｃｏ）を生成する。

暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、暗号化コンテンツ鍵Ｋｋ（Ｋｃｏ）は、認証鍵交換手段１９およびＤ－Ｉ／Ｆ１８を介して、それぞれＶＴＲ装置５へ伝達されるが、それに先だって、ＳＴＢ１、ＶＴＲ装置５それぞれの認証鍵交換手段１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

ＶＴＲ装置５へ伝達された暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、ＭＵＸ５４へ送られる。また、ＶＴＲ装置５へ伝達された暗号化コンテンツ鍵Ｋｋ（Ｋｃｏ）は、Ｄ－Ｉ／Ｆ５１および認証鍵交換手段５２を介して、鍵暗号解読手段６１に送られる。鍵暗号解読手段６１は、ＶＴＲ情報記憶手段７１に記憶されている共通鍵Ｋｋを用いて、暗号化コンテンツ鍵Ｋｋ（Ｋｃｏ）をコンテンツ鍵Ｋｃｏに復元して、鍵暗号化手段６２に送る。鍵暗号化手段６２は、ＶＴＲ情報記憶手段７１に記憶されているＳＴＢ１に固有の公開鍵 STBPａを用いて、コンテンツ鍵Ｋｃｏに暗号化を施して、暗号化コンテンツ鍵 STBPａ（Ｋｃｏ）を生成して、これをＭＵＸ５４へ送る。ＭＵＸ５４へ送られた暗号化ＡＶデータＫｃｏ（Ｄ）および暗号化コンテンツ鍵 STBPａ（Ｋｃｏ）は、記録媒体６のフォーマットに適合し

た多重化を行われた後、記録処理手段５５によって、記録媒体６に記録される。

次に、記録媒体６に記録されたＡＶデータを再生する時のデータの流れを図１２を用いて説明する。図１２は、本発明の第５の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図１２からわかるように、本実施の形態においては、記録された暗号化コンテンツ鍵 STBPａ（Ｋｃｏ）は、ＶＴＲ装置５内では復元されずに、ＳＴＢ１の鍵暗号解読手段１６へ送られ、ここで、ＳＴＢ情報記憶手段１７に記憶されているＳＴＢ１に固有の秘密鍵 STBSａを用いることによって、コンテンツ鍵Ｋｃｏに復元される。図１で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。すなわち、ＡＶデータを再生する時のデータの流れは、第１の実施の形態の図３と同じになる。

以上の手順にしたがって、ＡＶデータを記録／再生することにより、ＡＶデータの記録時において、ＶＴＲ装置５への送信側であるＳＴＢ１におけるコンテンツ鍵の暗号化が、負担の軽い共通鍵による暗号化としているので、ＡＶデータの暗号化およびコンテンツ鍵の暗号化を並行しておこなうことにより負担が増大しているＳＴＢ１の負担を軽減できるので、本実施の形態におけるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであり、かつ、第１の実施の形態におけるデータ記録再生システムと比較して、ＳＴＢ１およびＶＴＲ装置５の負担を平滑化して、記録効率の向上を図ることが可能なシステムであることがわかる。

なお、本発明の公開鍵および秘密鍵は、本実施の形態においては、第１の

実施の形態と同じく、本発明のチューナ装置（ＳＴＢ１）に対して固有な鍵であるとして説明したが、これに限るものではなく、例えば、第２～第４いずれかの実施の形態と同じく、本発明のチューナ装置（ＳＴＢ１）の機器モデルに対して固有な鍵、本発明のＩＣカードに記録されたユーザＩＤに対して固有な鍵、本発明のＩＣカードに記録されたサービスに対して固有な鍵であってもよい。

また、本発明の公開鍵の情報は、本実施の形態においては、ＶＴＲ情報記憶手段７１に記憶されているものとして説明したが、これに限るものではなく、例えば、記録を始める際に、ＳＴＢ１から送られてくるとしてもよい。

なお、本実施の形態におけるデータ記録再生システムから、図１３に示すように、鍵暗号化手段３１および鍵暗号解読手段６１を省略した構成も可能である。こうすれば、本発明のチューナ装置からＶＴＲ装置へのデータ送信において、コンテンツ鍵に暗号化を施さずに送信を行うことになる。このような構成は、後述する第８の実施の形態のように、ＳＴＢおよびＶＴＲ装置の機能を一体化した一体化ＳＴＢを備えるデータ記録再生システムに適用すると、特に有効である。以下に、図１３の構成のデータ記録再生システムについて説明する。

図１３の構成のデータ記録再生システムにおける、ＡＶデータを記録媒体６に記録する時のデータの流れは、図１４に示すようになる。図１４において、図１３で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。また、図中の記号については、図１１、図１２に倣う。

放送用電波として暗号化され、多重化されたＡＶデータＤは、アンテナ３を介して受信され、受信復調手段２１で復調され、放送用の暗号を放送用デ

スクランブル手段２０で解除され、ＤＭＵＸ２３で分離されて、生の(Plain)ＡＶデータＤとなって、映像デコーダ１１および音声デコーダ１２およびコンテンツ暗号化手段１３へ送られる。映像デコーダ１１および音声デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、ディスプレイ４へ出力する。コンテンツ暗号化手段１３は、コンテンツ鍵Ｋｃｏを生成し、生成したコンテンツ鍵Ｋｃｏを用いて、ＡＶデータＤに暗号化を施して、暗号化ＡＶデータＫｃｏ（Ｄ）を生成する。

暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、コンテンツ鍵Ｋｃｏは、認証鍵交換手段１９およびＤ－Ｉ／Ｆ１８を介して、それぞれＶＴＲ装置５へ伝達されるが、それに先だって、ＳＴＢ１、ＶＴＲ装置５それぞれの認証鍵交換手段１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

ＶＴＲ装置５へ伝達された暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、ＭＵＸ５４へ送られる。また、ＶＴＲ装置５へ伝達されたコンテンツ鍵Ｋｃｏは、Ｄ－Ｉ／Ｆ５１および認証鍵交換手段５２を介して、鍵暗号化手段６２に送られる。鍵暗号化手段６２は、ＶＴＲ情報記憶手段７１に記憶されているＳＴＢ１に固有の公開鍵 STBPａを用いて、コンテンツ鍵Ｋｃｏに暗号化を施して、暗号化コンテンツ鍵 STBPａ（Ｋｃｏ）を生成して、これをＭＵＸ５４へ送る。ＭＵＸ５４へ送られた暗号化ＡＶデータＫｃｏ（Ｄ）および暗号化コンテンツ鍵 STBPａ（Ｋｃｏ）は、記録媒体６のフォーマットに適合した多重化を行われた後、記録処理手段５５によって、記録媒体６に記録される。

図１３の構成のデータ記録再生システムにおける、データ再生時のデータの流れについては、図１２で示したデータ再生時のデータの流れと同じである。したがって、以下の説明を省略する。

なお、ＳＴＢ情報記憶手段１７およびＶＴＲ情報記憶手段７１は、図１０の構成において保持していた共通鍵の情報を保持している必要はない。

以上の手順にしたがって、ＡＶデータを記録／再生することにより、ＡＶデータの記録時において、ＶＴＲ装置５への送信側であるＳＴＢ１がコンテンツ鍵の暗号化を行わないので、ＡＶデータの暗号化およびコンテンツ鍵の暗号化を並行しておこなうことにより負担が増大しているＳＴＢ１の負担をさらに軽減できるので、図１３の構成のデータ記録再生システムは、図１０の構成のデータ記録再生システムと比較して、ＳＴＢ１およびＶＴＲ装置５の負担をさらに平滑化して、記録効率の向上を図ることが可能なシステムであることがわかる。ただし、図１０の構成のデータ記録再生システムと比較して、ＳＴＢ１からＶＴＲ装置５へのデータ送信についてのセキュリティは低下する。このような構成は、後述する第８の実施の形態のように、ＳＴＢおよびＶＴＲ装置の機能を一体化した一体化ＳＴＢを備えるデータ記録再生システムに適用すると、特に有効である。

（第６の実施の形態）

以下に、本発明の第６の実施の形態を図面を参照して説明する。本実施の形態が上述した第１の実施の形態と異なる点は、本発明の鍵暗号化手段および鍵暗号解読手段がＶＴＲ装置に備えられており、コンテンツ鍵の暗号化／復元を行う公開鍵／秘密鍵が、本発明のＶＴＲ装置に対して固有な鍵であることに関する点である。したがって、本実施の形態において、第１の実施の

形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第１の実施の形態と同じとする。

図１５は、本発明の第６の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムの構成が、第１の実施の形態におけるデータ記録再生システムの構成と異なるのは、本発明の鍵暗号化手段に対応する鍵暗号化手段６２および本発明の鍵暗号解読手段に対応する鍵暗号解読手段６４が、ＳＴＢ１ではなく、ＶＴＲ装置５に備えられており、それに伴い、ＳＴＢ１は、本発明の第二の鍵暗号化手段に対応する鍵暗号化手段３１および本発明の第二の鍵暗号解読手段に対応する鍵暗号解読手段３２を有し、ＶＴＲ装置５は、本発明の第二の鍵暗号解読手段に対応する鍵暗号解読手段６１と、本発明の第二の鍵暗号化手段に対応する鍵暗号化手段６３と、鍵暗号解読手段６１、鍵暗号化手段６２、鍵暗号化手段６３および鍵暗号解読手段６４が用いる共通鍵、公開鍵等の情報を記憶するＶＴＲ情報記憶手段７１とを有している。また、ＳＴＢ情報記憶手段１７は、第１の実施の形態において保持していた情報に加えて、鍵暗号化手段３１がコンテンツ鍵を暗号化するのに用いる共通鍵の情報を保持している。

なお、第１の実施の形態と同様に、課金情報が、例えば、ＳＴＢ情報記憶手段１７に記録される場合は、本実施の形態の構成におけるデータ記録再生システムから、ＩＣカード２およびカード読取手段１０を省いてもよい。

次に、このような本実施の形態の動作を説明する。

まず、ＡＶデータを記録媒体６に記録する時のデータの流れを図１４を用いて説明する。図１６は、本発明の第６の実施の形態におけるデータ記録再

生システムのデータ記録時のデータの流れを示すフロー図である。図１６において、図１５で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、図中の記号については、新たに説明するもの以外は、図２、図３に倣う。Ｋｋは、コンテンツ鍵Ｋｃｏの暗号化に用いるＳＴＢ１およびＶＴＲ装置５に共通な共通鍵を、Ｋｋ（Ｋｃｏ）は、コンテンツ鍵Ｋｃｏに共通鍵Ｋｋを用いて暗号化を施して得られる暗号化コンテンツ鍵を、 VTRＰａは、コンテンツ鍵Ｋｃｏの暗号化に用いるＶＴＲ装置５に固有の公開鍵を、 VTRＰａ（Ｋｃｏ）は、コンテンツ鍵Ｋｃｏに公開鍵 VTRＰａを用いて暗号化を施して得られる暗号化コンテンツ鍵を、それぞれ示す。なお、本実施の形態におけるデータ記録再生システムは、第１の実施の形態と同様に、コンテンツ鍵Ｋｃｏを、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

放送用電波として暗号化され、多重化されたＡＶデータＤは、アンテナ３を介して受信され、受信復調手段２１で復調され、放送用の暗号を放送用デスクランブル手段２０で解除され、ＤＭＵＸ２３で分離されて、生のＡＶデータＤとなって、映像デコーダ１１および音声デコーダ１２およびコンテンツ暗号化手段１３へ送られる。映像デコーダ１１および音声デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、ディスプレイ４へ出力する。コンテンツ暗号化手段１３は、コンテンツ鍵Ｋｃｏを生成し、生成したコンテンツ鍵Ｋｃｏを用いて、ＡＶデータＤに暗号化を施して、暗号化ＡＶデータＫｃｏ（Ｄ）を生成する。生成されたコンテンツ鍵Ｋｃｏは、鍵暗号化手段３１へ送られ、鍵暗号化手段３１は、ＳＴＢ情報記憶手段

１７に記憶されているＳＴＢ１およびＶＴＲ装置５に共通な共通鍵Ｋｋを用いて、コンテンツ鍵Ｋｃｏに暗号化を施して、暗号化コンテンツ鍵Ｋｋ（Ｋｃｏ）を生成する。

暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、暗号化コンテンツ鍵 STBPａ（Ｋｃｏ）は、認証鍵交換手段１９およびＤ－Ｉ／Ｆ１８を介して、それぞれＶＴＲ装置５へ伝達されるが、それに先だって、ＳＴＢ１、ＶＴＲ装置５それぞれの認証鍵交換手段１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

ＶＴＲ装置５へ伝達された暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、ＭＵＸ５４へ送られる。また、ＶＴＲ装置５へ伝達された暗号化コンテンツ鍵Ｋｋ（Ｋｃｏ）は、Ｄ－Ｉ／Ｆ５１および認証鍵交換手段５２を介して、鍵暗号解読手段６１に送られる。鍵暗号解読手段６１は、ＶＴＲ情報記憶手段７１に記憶されている共通鍵Ｋｋを用いて、暗号化コンテンツ鍵Ｋｋ（Ｋｃｏ）をコンテンツ鍵Ｋｃｏに復元して、鍵暗号化手段６２に送る。鍵暗号化手段６２は、ＶＴＲ情報記憶手段７１に記憶されているＶＴＲ装置５に固有の公開鍵 VTRＰａを用いて、コンテンツ鍵Ｋｃｏに暗号化を施して、暗号化コンテンツ鍵 VTRＰａ（Ｋｃｏ）を生成して、これをＭＵＸ５４へ送る。ＭＵＸ５４へ送られた暗号化ＡＶデータＫｃｏ（Ｄ）および暗号化コンテンツ鍵 VTRＰａ（Ｋｃｏ）は、記録媒体６のフォーマットに適合した多重化を行われた後、記録処理手段５５によって、記録媒体６に記録される。

次に、記録媒体６に記録されたＡＶデータを再生する時のデータの流れを

図１７を用いて説明する。図１７は、本発明の第６の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図１７において、図１５で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。 VTRＳａは、公開鍵 VTRＰａに対応し、暗号化コンテンツ鍵 VTRＰａ（Ｋｃｏ）を解読してコンテンツ鍵Ｋｃｏを復元するのに用いるＶＴＲ装置５に固有の秘密鍵を示す。図中の他の記号は、図１６に倣う。

多重化されて記録媒体６に記録された暗号化ＡＶデータＫｃｏ（Ｄ）および暗号化コンテンツ鍵 VTRＰａ（Ｋｃｏ）は、再生処理手段５８により再生され、ＤＭＵＸ５７で分離される。分離された暗号化コンテンツ鍵 VTRＰａ（Ｋｃｏ）は、鍵暗号解読手段６４へ送られる。鍵暗号解読手段６４は、ＶＴＲ情報記憶手段７１に記憶されているＶＴＲ装置５に固有の秘密鍵 VTRＳａを用いて、暗号化コンテンツ鍵 VTRＰａ（Ｋｗ）をコンテンツ鍵Ｋｃｏに復元して、鍵暗号化手段６３へ送る。鍵暗号化手段６３は、ＶＴＲ情報記憶手段７１に記憶されている共通鍵Ｋｋを用いて、コンテンツ鍵Ｋｃｏに暗号化を施して、暗号化コンテンツ鍵Ｋｋ（Ｋｃｏ）を生成する。

分離された暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、生成された暗号化コンテンツ鍵Ｋｋ（Ｋｃｏ）は、認証鍵交換手段５２およびＤ－Ｉ／Ｆ５１を介して、それぞれＳＴＢ１へ伝達されるが、それに先だって、記録時と同様に、ＳＴＢ１、ＶＴＲ装置５それぞれの認証鍵交換手段１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

ＳＴＢ１へ伝達された暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、コンテンツ暗号解読手段１４へ送られ、暗号化コンテンツ鍵Ｋｋ

（Ｋｃｏ）は、Ｄ－Ｉ／Ｆ１８および認証鍵交換手段１９を介して、鍵暗号解読手段３２へ送られる。鍵暗号解読手段３２は、ＳＴＢ情報記憶手段１７に記憶されている共通鍵Ｋｋを用いて、暗号化コンテンツ鍵Ｋｋ（Ｋｃｏ）をコンテンツ鍵Ｋｃｏに復元して、コンテンツ暗号解読手段１４へ送る。コンテンツ暗号解読手段１４は、復元されたコンテンツ鍵Ｋｃｏを用いて、暗号化ＡＶデータＫｃｏ（Ｄ）を解読して得られるＡＶデータＤを、映像デコーダ１１および音声デコーダ１２へ出力する。映像デコーダ１１および音声デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、ディスプレイ４へ出力する。

以上の手順にしたがって、ＡＶデータを記録／再生することにより、ＡＶデータに暗号化を施すのに用いたコンテンツ鍵にＶＴＲ装置５に固有の公開鍵を用いて暗号化を施して、暗号化されたＡＶデータと一緒に記録媒体に記録し、再生時には暗号化されたコンテンツ鍵をＶＴＲ装置５に固有の秘密鍵を用いて復元しているため、ＶＴＲ装置５に固有の秘密鍵を持っているシステム、すなわち、ＶＴＲ装置５そのものを備えているシステムしか再生できないので、本実施の形態におけるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであることがわかる。

なお、本実施の形態におけるデータ記録再生システムから、図１８に示すように、鍵暗号化手段３１、鍵暗号解読手段３２、鍵暗号解読手段６１および鍵暗号化手段６３を省略した構成も可能である。こうすれば、本発明のチューナ装置とＶＴＲ装置との間のデータ送信において、コンテンツ鍵に暗号化を施さずに送信を行うことになる。以下に、図１３の構成のデータ記録再

生システムについて説明する。

図１８の構成のデータ記録再生システムにおける、ＡＶデータを記録媒体６に記録する時のデータの流れは、図１９に示すようになる。図１９において、図１８で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。また、図中の記号については、図１６、図１７に倣う。

放送用電波として暗号化され、多重化されたＡＶデータＤは、アンテナ３を介して受信され、受信復調手段２１で復調され、放送用の暗号を放送用デスクランブル手段２０で解除され、ＤＭＵＸ２３で分離されて、生のＡＶデータＤとなって、映像デコーダ１１および音声デコーダ１２およびコンテンツ暗号化手段１３へ送られる。映像デコーダ１１および音声デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、ディスプレイ４へ出力する。コンテンツ暗号化手段１３は、コンテンツ鍵Ｋｃｏを生成し、生成したコンテンツ鍵Ｋｃｏを用いて、ＡＶデータＤに暗号化を施して、暗号化ＡＶデータＫｃｏ（Ｄ）を生成する。

暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、コンテンツ鍵Ｋｃｏは、認証鍵交換手段１９およびＤ－Ｉ／Ｆ１８を介して、それぞれＶＴＲ装置５へ伝達されるが、それに先だって、ＳＴＢ１、ＶＴＲ装置５それぞれの認証鍵交換手段１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

ＶＴＲ装置５へ伝達された暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、ＭＵＸ５４へ送られる。また、ＶＴＲ装置５へ伝達されたコンテンツ鍵Ｋｃｏは、Ｄ－Ｉ／Ｆ５１および認証鍵交換手段５２を介して、

鍵暗号化手段６２に送られる。鍵暗号化手段６２は、ＶＴＲ情報記憶手段７１に記憶されているＶＴＲ装置５に固有の公開鍵 VTRＰａを用いて、コンテンツ鍵Ｋｃｏに暗号化を施して、暗号化コンテンツ鍵 VTRＰａ（Ｋｃｏ）を生成して、これをＭＵＸ５４へ送る。ＭＵＸ５４へ送られた暗号化ＡＶデータＫｃｏ（Ｄ）および暗号化コンテンツ鍵 VTRＰａ（Ｋｃｏ）は、記録媒体６のフォーマットに適合した多重化を行われた後、記録処理手段５５によって、記録媒体６に記録される。

次に、図１８の構成のデータ記録再生システムにおける、記録媒体６に記録されたＡＶデータを再生する時のデータの流れを図２０を用いて説明する。図２０において、図１８で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。また、図中の記号については、図１６、図１７に倣う。

多重化されて記録媒体６に記録された暗号化ＡＶデータＫｃｏ（Ｄ）および暗号化コンテンツ鍵 VTRＰａ（Ｋｃｏ）は、再生処理部手段５８により再生され、ＤＭＵＸ５７で分離される。分離された暗号化コンテンツ鍵 VTRＰａ（Ｋｃｏ）は、鍵暗号解読手段６４へ送られる。鍵暗号解読手段６４は、ＶＴＲ情報記憶手段７１に記憶されているＶＴＲ装置５に固有の秘密鍵 VTRＳａを用いて、暗号化コンテンツ鍵 VTRＰａ（Ｋｃｏ）をコンテンツ鍵Ｋｃｏに復元する。

分離された暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、復元されたコンテンツ鍵Ｋｃｏは、認証鍵交換手段５２およびＤ－Ｉ／Ｆ５１を介して、それぞれＳＴＢ１へ伝達されるが、それに先だって、記録時と同様に、ＳＴＢ１、ＶＴＲ装置５それぞれの認証鍵交換手段１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な

相手であることを確認した上で、前記伝達が行われる。

ＳＴＢ１へ伝達された暗号化ＡＶデータＫｃｏ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、コンテンツ暗号解読手段１４へ送られ、コンテンツ鍵Ｋｃｏは、Ｄ－Ｉ／Ｆ１８および認証鍵交換手段１９を介して、それぞれコンテンツ暗号解読手段１４へ送られる。コンテンツ暗号解読手段１４は、コンテンツ鍵Ｋｃｏを用いて、暗号化ＡＶデータＫｃｏ（Ｄ）を解読して得られるＡＶデータＤを、映像デコーダ１１および音声デコーダ１２へ出力する。映像デコーダ１１および音声デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、ディスプレイ４へ出力する。

なお、ＳＴＢ情報記憶手段１７およびＶＴＲ情報記憶手段７１は、図１５の構成において保持していた共通鍵の情報を保持している必要はない。

以上の手順にしたがって、ＡＶデータを記録／再生することにより、ＳＴＢ１とＶＴＲ装置５との間のデータ送信において、コンテンツ鍵に暗号化を施さずに送信を行うので、記録／再生時のＳＴＢ１およびＶＴＲ装置５の負担をさらに軽減できるので、図１８の構成のデータ記録再生システムは、図１５の構成のデータ記録再生システムと比較して、さらに記録効率の向上を図ることが可能なシステムであることがわかる。ただし、図１５の構成のデータ記録再生システムと比較して、ＳＴＢ１とＶＴＲ装置５との間のデータ送信についてのセキュリティは低下する。このような構成は、後述する第８の実施の形態のように、ＳＴＢおよびＶＴＲ装置の機能を一体化した一体化ＳＴＢを備えるデータ記録再生システムに適用すると、特に有効である。

（第７の実施の形態）

以下に、本発明の第７の実施の形態を図面を参照して説明する。本実施の

形態が上述した第１の実施の形態と異なる点は、公開鍵および秘密鍵を用いる替わりに、共通鍵を用いてコンテンツ鍵の暗号化／復元を行う点である。したがって、本実施の形態において、第１の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第１の実施の形態と同じとする。

本実施の形態におけるデータ記録再生システムの構成は、第１の実施の形態におけるデータ記録再生システムの構成と同じである。

次に、このような本実施の形態の動作を説明する。

図２１は、本発明の第７の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図であり、図２２は、本発明の第７の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図２１、図２２に示すとおり、本実施の形態においては、コンテンツ鍵Ｋｃｏの暗号化および復元にＳＴＢ情報記憶手段１７に保持されている共通鍵Ｋｋを用いている点以外は、第１の実施の形態におけるデータ記録再生システムと同じである。なお、共通鍵Ｋｋは、例えば、ＳＴＢ１もしくはＳＴＢ１の機器モデル、ユーザＩＤ、サービスいずれかに対して固有な鍵である。また、共通鍵Ｋｋは、ＩＣカード２に記録されているとしてもよい。共通鍵ＫｋがＩＣカード２に記録されていない場合で、課金情報が、例えば、ＳＴＢ情報記憶手段１７に記録される場合は、カード読取手段１０を省略してもよい。また、共通鍵ＫｋがＳＴＢ記憶手段１１に記録されていない場合は、ＳＴＢ記憶手段１１を省略してもよい。

以上の手順にしたがって、ＡＶデータを記録／再生することにより、コンテンツ鍵に暗号化に公開鍵を用いないので、本実施の形態におけるデータ記

録再生システムは、第１の実施の形態におけるデータ記録再生システムと比較して、鍵自身のデータ長を短くでき、記録効率の向上および装置の小型化を図ることが可能なシステムであることがわかる。

（第８の実施の形態）

以下に、本発明の第８の実施の形態を図面を参照して説明する。本実施の形態が上述した第１の実施の形態と異なる点は、第１の実施の形態におけるデータ記録再生システムが本発明のチューナ装置およびＶＴＲ装置を備えていたのに対し、本実施の形態におけるデータ記録再生システムが前記チューナ装置および前記ＶＴＲ装置の機能が一体化された装置を備えていることに関する点である。したがって、本実施の形態において、第１の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第１の実施の形態と同じとする。

図２３は、本発明の第８の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムの構成が、第１の実施の形態におけるデータ記録再生システムの構成と異なるのは、ＳＴＢ１およびＶＴＲ装置５の機能を一体化した一体化ＳＴＢ７を備えることによって、第１の実施の形態におけるデータ記録再生システムが備えていたＤ－Ｉ／Ｆ１８および５１を省略したことである。

なお、第１の実施の形態と同様に、課金情報が、例えば、ＳＴＢ情報記憶手段１７に記録される場合は、本実施の形態の構成におけるデータ記録再生システムから、ＩＣカード２およびカード読取手段１０を省いてもよい。

次に、このような本実施の形態の動作を説明する。

まず、ＡＶデータを記録媒体６に記録する時のデータの流れを図２４を用

いて説明する。図２４は、本発明の第８の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。図２４において、図２３で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、図中の記号については、図２、図３に倣うが、 STBＰａは、コンテンツ鍵Ｋｃｏの暗号化に用いる一体化ＳＴＢ７に固有の公開鍵を示す。なお、本実施の形態におけるデータ記録再生システムは、第１の実施の形態と同様に、コンテンツ鍵Ｋｃｏを、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

放送用電波として暗号化され、多重化されたＡＶデータＤは、アンテナ３を介して受信され、受信復調手段２１で復調され、放送用の暗号を放送用デスクランブル手段２０で解除され、ＤＭＵＸ２３で分離されて、生のＡＶデータＤとなって、映像デコーダ１１および音声デコーダ１２およびコンテンツ暗号化手段１３へ送られる。映像デコーダ１１および音声デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、ディスプレイ４へ出力する。コンテンツ暗号化手段１３は、コンテンツ鍵Ｋｃｏを生成し、生成したコンテンツ鍵Ｋｃｏを用いて、ＡＶデータＤに暗号化を施して、暗号化ＡＶデータＫｃｏ（Ｄ）を生成する。生成されたコンテンツ鍵Ｋｃｏは、鍵暗号化手段１５へ送られ、鍵暗号化手段１５は、ＳＴＢ情報記憶手段１７に記憶されている一体化ＳＴＢ７に固有の公開鍵 STBＰａを用いて、コンテンツ鍵Ｋｃｏに暗号化を施して、暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ）を生成する。

生成された暗号化ＡＶデータＫｃｏ（Ｄ）および暗号化コンテンツ鍵 STB

Ｐａ（Ｋｃｏ）は、それぞれＭＵＸ５４へ送られて、記録媒体６のフォーマットに適合した多重化を行われた後、記録処理手段５５によって、記録媒体６に記録される。

次に、記録媒体６に記録されたＡＶデータを再生する時のデータの流れを図２５を用いて説明する。図２５は、本発明の第８の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図２５において、図２３で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。図中の記号は、図２、図３に倣うが、 STBＳａは、公開鍵 STBＰａに対応し、暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ）を解読してコンテンツ鍵Ｋｃｏを復元するのに用いる一体化ＳＴＢ７に固有の秘密鍵を示す。

多重化されて記録媒体６に記録された暗号化ＡＶデータＫｃｏ（Ｄ）および暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ）は、再生処理部手段５８により再生され、ＤＭＵＸ５７で分離される。

分離された暗号化ＡＶデータＫｃｏ（Ｄ）は、コンテンツ暗号解読手段１４へ送られ、分離された暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ）は、鍵暗号解読手段１６へ送られる。鍵復元手段１６は、ＳＴＢ情報記憶手段１７に記憶されている一体化ＳＴＢ７に固有の秘密鍵 STBＳａを用いて、暗号化コンテンツ鍵 STBＰａ（Ｋｃｏ）をコンテンツ鍵Ｋｗに復元して、コンテンツ暗号解読手段１４へ送る。コンテンツ暗号解読手段１４は、復元されたコンテンツ鍵Ｋｃｏを用いて、暗号化ＡＶデータＫｃｏ（Ｄ）を解読して得られるＡＶデータＤを、映像デコーダ１１および音声デコーダ１２へ出力する。映像デコーダ１１および音声デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、ディスプレイ４へ出力する。

以上の手順にしたがって、ＡＶデータを記録／再生することにより、各装置間のデータ伝達にかかる負担を省略できるので、本実施の形態におけるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであり、かつ、第１の実施の形態におけるデータ記録再生システムと比較して、さらに記録効率の向上を図ることが可能なシステムであることがわかる。

なお、本発明の公開鍵および秘密鍵は、本実施の形態においては、一体化ＳＴＢ７に対して固有な鍵であるとして説明したが、これに限るものではなく、例えば、第２～第４いずれかの実施の形態と同様に、一体化ＳＴＢ７の機器モデルに対して固有な鍵、本発明のＩＣカードに記録されたユーザＩＤに対して固有な鍵、本発明のＩＣカードに記録されたサービスに対して固有な鍵であってもよい。

なお、本発明のコンテンツ鍵は、上述した第１～第８の実施の形態においては、定期的または不定期的に切り替えられるとして説明したが、同じコンテンツ鍵を用いるとすると、定期的または不定期的に切り替える場合と比較して、暗号化に関する情報が外部に漏洩するおそれが高くなるが、従来のデータ記録再生システムと比較すると、暗号化に関する情報が外部に漏洩しにくいシステムであるといえる。

また、本発明の第２の暗号化は、上述した第１～第８の実施の形態においては、本発明の第１の暗号化において用いたコンテンツ鍵とは別の鍵（公開鍵、共通鍵）であるとして説明したが、これに限るものではなく、第１の暗号化に用いたコンテンツ鍵に対応するアルゴリズムと同じアルゴリズムを用いて、当該コンテンツ鍵自身に第２の暗号化を施すとしてもよい。また、例

えば、コンテンツ鍵として共通鍵を用いてディジタルデータに第１の暗号化を施し、当該共通鍵に同じ共通鍵を用いて第２の暗号化を施すとしてもよい。なお、上述した第１～第８の実施の形態においては、本発明のデータ記録再生システムを中心に説明したが、本発明のデータ記録再生方法は、上記説明中で、説明された方法である。

（第９の実施の形態）

先ず、本発明の第９の実施の形態の記録装置および再生装置の構成を述べる。

図２６に、本発明の第９の実施の形態の記録装置および再生装置のブロック図を示す。本発明の第９の実施の形態の記録装置は、第１鍵発生手段８０と、コンテンツ暗号化手段１３と、第２鍵発生手段８１と、ＫｘＦＩＦＯ８５と、鍵暗号化手段７０と、対応関係情報生成手段８４と、ＭＵＸ５４から構成される。また、本発明の第９の実施の形態の再生装置は、ＤＭＵＸ５７と、鍵暗号化鍵取得手段８２と、Ｋｘラッチ手段８６と、鍵暗号解読手段７１と、コンテンツ暗号解読手段１４から構成される。なお、図２６には、受信復調手段２１と、ＤＭＵＸ２３と、ＥＭＭ解読手段２５と、ＥＣＭ解読手段２４と、放送デスクランブル手段２０と、映像デコーダ１１と、音声デコーダ１２も表示する。さらに、記録媒体としての記録媒体６と、映像を表示し、音声を出力するディスプレイ４も表示する。

受信復調手段２１は、放送局からの、デジィタルの映像データ、音声データ、ＥＭＭ（個別情報）、ＥＣＭ（番組情報）および暗号化された放送スクランブル鍵Ｋｓを通信衛星を介して入力し、それらの全部または一部の信号波形を整形する手段である。

さて、ＤＭＵＸ２３は、受信復調手段２１からの、波形整形された映像データ、音声データ、ＥＭＭ、ＥＣＭおよび暗号化された放送スクランブル鍵Ｋｓを分離する手段であるとともに、放送デスクランブル手段２０からの、デスクランブルされた映像データおよび音声データを分離する手段である。また、ＤＭＵＸ２３は、コンテンツ暗号解読手段１４からの映像データおよび音声データを分離する手段でもある。

ＥＭＭ解読手段２５は、ユーザＩＤ鍵Ｋｍを入力するとともに、ＤＭＵＸ２３からのＥＭＭを入力し、ユーザＩＤ鍵ＫｍでＥＭＭを解読してワーク鍵Ｋｗを生成する手段である。

ＥＣＭ解読手段２４は、ＥＭＭ解読手段２５からのワーク鍵Ｋｗを入力するとともに、ＤＭＵＸ２３からのＥＣＭおよび暗号化された放送スクランブル鍵Ｋｓを入力し、ワーク鍵ＫｗでＥＣＭを解読して放送スクランブル鍵Ｋｓを復元する手段である。

放送デスクランブル手段２０は、ＥＣＭ解読手段２４からの放送スクランブル鍵Ｋｓを入力するとともに、ＤＭＵＸ２３からの、スクランブルされたＡＶデータを入力し、放送スクランブル鍵Ｋｓで、スクランブルされたＡＶデータをデスクランブルする手段である。

第１鍵発生手段８０は、放送デスクランブル手段２０によってデスクランブルされたＡＶデータを、再度暗号化するためのコンテンツ鍵Ｋｃｏを発生する手段である。

コンテンツ暗号化手段１３は、放送デスクランブル手段２０からのＡＶデータＤを入力するとともに、第１鍵発生手段８０からのコンテンツ鍵Ｋｃｏを入力し、そのコンテンツ鍵ＫｃｏでＡＶデータＤを暗号化する手段である。

なお、以下では、コンテンツ鍵Ｋｃｏにより暗号化されたＡＶデータＤをＫｃｏ（Ｄ）とする。

第２鍵発生手段８１は、第１鍵発生手段８０が発生したコンテンツ鍵Ｋｃｏを暗号化するための鍵暗号化鍵Ｋｘを発生する手段である。なお、第２鍵発生手段８１は、毎日異なる鍵暗号化鍵Ｋｘを発生するものとし、それら異なるＫｘをそれぞれＫｘ１、Ｋｘ２、Ｋｘ３、…とする。また、鍵暗号化鍵Ｋｘ１、Ｋｘ２、Ｋｘ３、…それぞれは、１週間で廃棄されるものであるとする。

ＫｘＦＩＦＯ８５は、第２鍵発生手段８１からの鍵暗号化鍵Ｋｘ１、Ｋｘ２、Ｋｘ３、…を入力し格納する手段であるとともに、タイマーを有していて、そのタイマーを利用して、入力後１週間経過した鍵暗号化鍵Ｋｘを廃棄する、ファーストインファーストアウト機能を有する手段である。

鍵暗号化手段７０は、第１鍵発生手段８０からのコンテンツ鍵Ｋｃｏを入力するとともに、ＫｘＦＩＦＯ８５からの鍵暗号化鍵Ｋｘを入力し、その鍵暗号化鍵Ｋｘでコンテンツ鍵Ｋｃｏを暗号化する手段である。なお、以下では、鍵暗号化鍵Ｋｘにより暗号化されたコンテンツ鍵ＫｃｏをＫｘ（Ｋｃｏ）とする。

対応関係情報生成手段８４は、コンテンツ鍵Ｋｃｏにより暗号化されたＡＶデータＫｃｏ（Ｄ）と、そのコンテンツ鍵Ｋｃｏを暗号化した鍵暗号化鍵Ｋｘとを対応付けるための情報として、鍵暗号化鍵Ｋｘ４が発生された日時の情報を生成する手段である。

ＭＵＸ５４は、コンテンツ暗号化手段１３からの暗号化されたＡＶデータＫｃｏ（Ｄ）と、鍵暗号化手段７０からのＫｘ（Ｋｃｏ）と、対応関係情報

生成手段８４からの日時情報とを入力し、それらを記録媒体６に記録する手段である。

ＤＭＵＸ５７は、記録媒体６に記録された、暗号化されたＡＶデータＫｃｏ（Ｄ）、Ｋｘ（Ｋｃｏ）および日時情報を入力し、それらを分離する手段である。

鍵暗号化鍵取得手段８２は、ＤＭＵＸ５７からの日時情報を入力し、その日時情報に基づいて、再生しようとする暗号化されたＡＶデータＫｃｏ（Ｄ）に対応する鍵暗号化鍵Ｋｘを特定し、その特定した鍵暗号化鍵ＫｘをＫｘＦＩＦＯ８５のなかから取得する手段である。

Ｋｘラッチ手段８６は、鍵暗号化鍵取得手段８２からの鍵暗号化鍵Ｋｘを入力してラッチし、鍵暗号解読手段７１に出力する手段である。

鍵暗号解読手段７１は、ＤＭＵＸ５７からのＫｘ（Ｋｃｏ）を入力するとともに、Ｋｘラッチ手段８６からの鍵暗号化鍵Ｋｘを入力し、その鍵暗号化鍵ＫｘでＫｘ（Ｋｃｏ）を解読し、コンテンツ鍵Ｋｃｏを復元する手段である。

コンテンツ暗号解読手段１４は、ＤＭＵＸ５７からの暗号化されたＡＶデータＫｃｏ（Ｄ）を入力するとともに、鍵暗号解読手段７１からのコンテンツ鍵Ｋｃｏを入力し、そのコンテンツ鍵Ｋｃｏで暗号化されたＡＶデータＫｃｏ（Ｄ）を暗号解読する手段である。

映像デコーダ１１は、ＤＭＵＸ２３からの映像データを復号する手段である。

音声デコーダ１２は、ＤＭＵＸ２３からの音声データを復号する手段である。

なお、請求項３９の本発明の、コンテンツ暗号化手段としてコンテンツ暗号化手段１３、鍵暗号化鍵発生手段として第２鍵発生手段８１、格納手段としてＫｘＦＩＦＯ８５、鍵暗号化手段として鍵暗号化手段７０、対応関係情報生成手段として対応関係情報生成手段８４、記録手段としてＭＵＸ５４を用いた。また、請求項４４の本発明のコンテンツ鍵発生手段として第１鍵発生手段８０を、本実施の形態では用いた。さらに、請求項４５の本発明の、鍵暗号化鍵取得手段として鍵暗号化鍵取得手段８２、鍵暗号解読手段として鍵暗号解読手段７１、コンテンツ暗号解読手段としてコンテンツ暗号解読手段１４を用いた。

次に、このような本発明の第９の実施の形態の記録装置の動作を述べる。

先ず、受信復調手段２１は、放送局からの、デジィタルの映像データ、音声データ、ＥＭＭ（個別情報）、ＥＣＭ（番組情報）および暗号化された放送スクランブル鍵Ｋｓを入力し、映像データおよび音声データの信号波形の乱れを整形し、映像データ、音声データ、ＥＭＭ、ＥＣＭおよび暗号化された放送スクランブル鍵ＫｓをＤＭＵＸ２３に出力する。

その後、ＤＭＵＸ２３は、受信復調手段２１からの映像データ、音声データ、ＥＭＭ、ＥＣＭおよび放送スクランブル鍵Ｋｓを入力して分離し、映像データおよび音声データ（ＡＶデータ）を放送デスクランブル手段２０に出力する。また、ＥＭＭをＥＭＭ解読手段２５に出力し、ＥＣＭおよび暗号化された放送スクランブル鍵ＫｓをＥＣＭ解読手段２４に出力する。

次に、ＥＭＭ解読手段２５は、ユーザＩＤ鍵Ｋｍを入力するとともに、ＤＭＵＸ２３からのＥＭＭを入力し、ユーザＩＤ鍵ＫｍでＥＭＭを解読してワーク鍵Ｋｗを生成し、ＥＣＭ解読手段２４に出力する。

さらに、ＥＣＭ解読手段２４は、ＥＭＭ解読手段２５からのワーク鍵Ｋｗを入力するとともに、ＤＭＵＸ２３からの、ＥＣＭおよび暗号化された放送スクランブル鍵Ｋｓを入力し、ワーク鍵ＫｗでＥＣＭを解読して、暗号化された放送スクランブル鍵Ｋｓの暗号化を復元し、放送デスクランブル手段２０に出力する。

そして、放送デスクランブル手段２０は、ＥＣＭ解読手段２４からの放送スクランブル鍵Ｋｓを入力するとともに、ＤＭＵＸ２３からの、スクランブルされたＡＶデータを入力し、放送スクランブル鍵Ｋｓで、スクランブルされたＡＶデータをデスクランブルする。そして、放送デスクランブル手段２０は、デスクランブルされたＡＶデータをＤＭＵＸ２３またはコンテンツ暗号化手段１３に出力する。なお、放送デスクランブル手段２０は、リアルタイムでＡＶデータを直接ディスプレイ４に表示させる場合にＤＭＵＸ２３に出力し、記録媒体６にＡＶデータを記録させる場合にコンテンツ暗号化手段１３に出力する。ただし、記録媒体６に記録されるＡＶデータは、放送デスクランブル手段２０からの、そのままのＡＶデータではなく、再度コンテンツ暗号化されたデータである。

はじめに、放送デスクランブル手段２０がＡＶデータをＤＭＵＸ２３に出力する場合について説明する。

その場合、ＤＭＵＸ２３は、放送デスクランブル手段２０からのＡＶデータを入力し、それを映像データと音声データに分離して、映像データを映像デコーダ１１に出力し、音声データを音声デコーダ１２に出力する。その後、映像デコーダ１１および音声デコーダ１２それぞれは、ＤＭＵＸ２３からの映像データまたは音声データを復号し、ディスプレイ４に出力する。そし

て、ディスプレイ４は、映像を表示し音声を出力する。

次に、放送デスクランブル手段２０がＡＶデータをコンテンツ暗号化手段１３に出力する場合について説明する。つまり、上述したように、記録媒体６にＡＶデータを記録する場合である。

先ず、コンテンツ暗号化手段１３は、放送デスクランブル手段２０からの、デスクランブルされたＡＶデータＤを入力する。

そして、第１鍵発生手段８０は、コンテンツ暗号化手段１３が入力したＡＶデータＤを暗号化するためのコンテンツ鍵Ｋｃｏを発生し、コンテンツ暗号化手段１３および鍵暗号化手段７０に出力する。

次に、コンテンツ暗号化手段１３は、第１鍵発生手段８０からのコンテンツ鍵Ｋｃｏを入力し、そのコンテンツ鍵ＫｃｏでＡＶデータＤを暗号化する。つまり、Ｋｃｏ（Ｄ）を生成する。そして、Ｋｃｏ（Ｄ）を対応関係情報生成手段８４およびＭＵＸ５４に出力する。

他方、第２鍵発生手段８１は、第１鍵発生手段８０が発生したコンテンツ鍵Ｋｃｏを暗号化するための鍵暗号化鍵Ｋｘを発生する。その第２鍵発生手段８１が発生する鍵暗号化鍵Ｋｘは毎日異なるものとする。ここでは、以下の説明の便宜上、記録装置が動作し始める日を１９９８年１月１日であるとし、記録時である本日をその日から３日後の１９９８年１月４日であるとし、図２７の鍵暗号化鍵Ｋｘリスト（ａ）に示すように、１月１日に発生された鍵暗号化鍵ＫｘをＫｘ１、１月２日に発生された鍵暗号化鍵ＫｘをＫｘ２、…、１月４日に発生された鍵暗号化鍵ＫｘをＫｘ４とする。また、以下、同様にして鍵暗号化鍵Ｋｘは発生されるものとする。なお、ことわりがない限り、以下、１月４日の記録装置の動作について説明する。

さて、ＫｘＦＩＦＯ８５は、図２７（ａ）のリストに示すように、１月１日から毎日一つづつの鍵暗号化鍵Ｋｘを第２鍵発生手段８１から既に入力して格納し、１月３日までに鍵暗号化鍵Ｋｘ１、Ｋｘ２、Ｋｘ３を格納しておき、本日１月４日には、Ｋｘ４を入力して格納する。その格納は、常に最新の鍵暗号化鍵Ｋｘが図２７（ａ）のリストのトップの順位にくるように行われ、また、古いものは順次順位を下げるように行われる。なお、ＫｘＦＩＦＯ８５は、格納した鍵暗号化鍵Ｋｘ１、Ｋｘ２、…を、それぞれの格納から１週間経過した後に廃棄する。例えば、図２７（ｂ）のリストに示すように、１月９日になると、Ｋｘ１、Ｋｘ２という鍵暗号化鍵は廃棄され、ＫｘＦＩＦＯ８５は、Ｋｘ９、Ｋｘ８、…、Ｋｘ４、Ｋｘ３という順序で７つの鍵暗号化鍵を格納することになる。つまり、ＫｘＦＩＦＯ８５が格納する鍵暗号化鍵Ｋｘの数は７までである。

次に、鍵暗号化手段７０は、第１鍵発生手段８０からのコンテンツ鍵Ｋｃｏを入力するとともに、ＫｘＦＩＦＯ８５を介して、第２鍵発生手段８１が記録時である１月４日に発生した鍵暗号化鍵Ｋｘ４を入力し、その鍵暗号化鍵Ｋｘ４でコンテンツ鍵Ｋｃｏを暗号化する。つまり、Ｋｘ４（Ｋｃｏ）を生成する。

そして、対応関係情報生成手段８４は、コンテンツ暗号化手段１３からの暗号化されたＡＶデータＫｃｏ（Ｄ）と、鍵暗号化手段７０からのＫｘ４（Ｋｃｏ）とを入力し、その鍵暗号化鍵Ｋｘ４と、その鍵暗号化鍵Ｋｘ４で暗号化されたコンテンツ鍵Ｋｃｏにより暗号化されたＡＶデータＫｃｏ（Ｄ）とを対応付けるための情報として、その鍵暗号化鍵Ｋｘ４が発生された日時の情報を生成する。つまり、１月４日という日時情報を生成する。

その後、ＭＵＸ５４は、コンテンツ暗号化手段１３からの暗号化されたＡＶデータＫｃｏ（Ｄ）と、鍵暗号化手段７０からのＫｘ４（Ｋｃｏ）と、対応関係情報生成手段８４からの１月４日という日時情報とを入力し、それらを１組として記録媒体６に記録する。

このようにして、毎日、その日に発生された鍵暗号化鍵Ｋｘｎ（ｎ＝１、２、…）に対応するＫｘｎ（Ｋｃｏ）と、暗号化されたＡＶデータＫｃｏ（Ｄ）と、その日の日時情報とが１組となって記録媒体６に記録される。

次に、本発明の第９の実施の形態の再生装置の動作を述べる。

つまり、記録装置によって記録媒体６に記録された暗号化されたＡＶデータＫｃｏ（Ｄ）を再生する場合について説明する。

以下の説明の便宜上、再生装置が記録媒体６の暗号化されたＡＶデータＫｃｏ（Ｄ）を再生する日を１月９日であるとする。そして、再生装置は、１月１日に記録媒体６に記録された暗号化されたＡＶデータＫｃｏ（Ｄ）と、１月３日に記録媒体６に記録された暗号化されたＡＶデータＫｃｏ（Ｄ）とを再生しようとするものとする。

はじめに、再生装置が１月１日に記録媒体６に記録された暗号化されたＡＶデータＫｃｏ（Ｄ）を再生しようとする場合について説明する。

先ず、ＤＭＵＸ５７は、記録媒体６からの、１月１日に記録された暗号化されたＡＶデータＫｃｏ（Ｄ）と、Ｋｘ１（Ｋｃｏ）と、１月１日という日時情報とを入力し、それらを分離し、１月１日という日時情報を鍵暗号化鍵取得手段８２に出力する。

そして、鍵暗号化鍵取得手段８２は、その１月１日という日時情報を入力し、その日時情報に基づいて、鍵暗号化鍵Ｋｘ１を特定し、ＫｘＦＩＦＯ８

５が格納している、図２７（ｂ）のリストのなかから鍵暗号化鍵Ｋｘ１を検索する。しかしながら、その鍵暗号化鍵Ｋｘ１は、発生から一週間以上経過しているので、ＫｘＦＩＦＯ８５により廃棄されており、図２７（ｂ）のリストのなかには存在しない。したがって、鍵暗号化鍵取得手段８２は、鍵暗号鍵Ｋｘ１を取得することができない。その結果、コンテンツ暗号解読手段１４は、その鍵暗号鍵Ｋｘ１を間接的に用いて暗号解読する必要がある、１月１日に記録された暗号化されたＡＶデータＫｃｏ（Ｄ）を暗号解読することができなくなり、そのＡＶデータがディスプレイ４に出力されても、解読不能なため、ディスプレイ４は、ＡＶデータ本来の映像および音声を出力することができない。

次に、再生装置が１月３日に記録媒体６に記録された暗号化されたＡＶデータＫｃｏ（Ｄ）を再生しようとする場合について説明する。

先ず、ＤＭＵＸ５７は、記録媒体６からの、１月３日に記録された暗号化されたＡＶデータＫｃｏ（Ｄ）と、Ｋｘ３（Ｋｃｏ）と、１月３日という日時情報とを入力し、それらを分離し、１月３日という日時情報を鍵暗号鍵取得手段１４に出力する。

次に、鍵暗号鍵取得手段１４は、その１月３日という日時情報を入力し、その日時情報に基づいて、鍵暗号鍵Ｋｘ３を特定し、ＫｘＦＩＦＯ８５が格納している、図２７（ｂ）のリストのなかから鍵暗号鍵Ｋｘ３を検索してその鍵暗号化鍵Ｋｘ３を取得し、それをＫｘラッチ手段８６に出力する。

その後、Ｋｘラッチ手段８６は、鍵暗号化鍵Ｋｘ３を入力し、鍵暗号解読手段７１に出力する。また、ＤＭＵＸ５７は、Ｋｘ３（Ｋｃｏ）を鍵暗号解読手段７１に出力する。

そして、鍵暗号解読手段７１は、ＤＭＵＸ５７からのＫｘ３（Ｋｃｏ）を入力するとともに、Ｋｘラッチ手段８６からの鍵暗号化鍵Ｋｘ３を入力し、その鍵暗号化鍵Ｋｘ３でＫｘ３（Ｋｃｏ）を解読し、コンテンツ鍵Ｋｃｏを復元して、そのコンテンツ鍵Ｋｃｏをコンテンツ暗号解読手段１４に出力する。また、ＤＭＵＸ５７は、暗号化されたＡＶデータＫｃｏ（Ｄ）を鍵暗号解読手段７１に出力する。

次に、コンテンツ暗号解読手段１４は、ＤＭＵＸ５７からの暗号化されたＡＶデータＫｃｏ（Ｄ）を入力するとともに、鍵暗号解読手段７１からのコンテンツ鍵Ｋｃｏを入力し、そのコンテンツ鍵Ｋｃｏで暗号化されたＡＶデータＫｃｏ（Ｄ）を暗号解読して、その暗号解読されたＡＶデータをＤＭＵＸ２３に出力する。

そして、ＤＭＵＸ２３は、コンテンツ暗号解読手段１４からのＡＶデータＤを入力し、それを映像データと音声データに分離して、映像データを映像デコーダ１１に出力し、音声データを音声デコーダ１２に出力する。その後、映像デコーダ１１および音声デコーダ１２それぞれは、ＤＭＵＸ２３からの映像データまたは音声データを復号し、ディスプレイ４に出力する。そして、ディスプレイ４は、映像を表示し音声を出力する。

このようにして、記録媒体６に記録された暗号化されたＡＶデータＫｃｏ（Ｄ）それぞれは、記録されてから１週間以内でないと、最終的に、本来の映像および音声として再生されない。

なお、上述した第９の実施の形態では、記録媒体６に記録された暗号化されたＡＶデータＫｃｏ（Ｄ）それぞれは、記録されてから１週間以内であれば再生されるとしたが、１週間以内というような期間の制限ではなく、暗号

化されたＡＶデータＫｃｏ（Ｄ）それぞれの再生回数を、例えば１回や３回というように制限して、その制限再生回数内でないと、再生されないとしてもよい。つまり、図２８に示すように、本発明の再生装置がカウンタ８７を備え、そのカウンタ８７が各暗号化されたＡＶデータＫｃｏ（Ｄ）の再生回数をチェックし、例えば１回や３回というような制限された再生回数に達した場合、ＫｘＦＩＦＯ８５が、その暗号化されたＡＶデータＫｃｏ（Ｄ）に対応する鍵暗号化鍵Ｋｘを廃棄するとしてもよい。また、上述した１週間以内というような期間の制限と再生回数の制限を併用するとしてもよい。

また、上述した第９の実施の形態では、ＫｘＦＩＦＯ８５は、格納した鍵暗号化鍵Ｋｘを１週間経過した後に廃棄するとした。しかし、ＫｘＦＩＦＯ８５は、格納した鍵暗号化鍵Ｋｘを１週間経過しても廃棄せずに、格納したままにしておき、鍵暗号化鍵取得手段８２が、暗号化されたＡＶデータＫｃｏ（Ｄ）を再生しようとする日が鍵暗号化鍵Ｋｘの発生から１週間以内か否かを判断して、または、制限回数内か否かを判断して、１週間以内または制限回数内以内であれば、再生しようとする暗号化されたＡＶデータＫｃｏ（Ｄ）に対応する鍵暗号化鍵ＫｘをＫｘＦＩＦＯ８５から取得できるとしてもよい。したがって、この場合、請求項４６の本発明では、コンテンツ暗号化手段としてコンテンツ暗号化手段１３、鍵暗号化鍵発生手段として第２鍵発生手段８１、格納手段としてＫｘＦＩＦＯ８５、鍵暗号化手段として鍵暗号化手段７０、対応関係情報生成手段として対応関係情報生成手段８４、記録手段としてＭＵＸ５４がそれぞれ該当することになる。また、請求項５０の本発明では、鍵暗号化鍵取得手段として鍵暗号化鍵取得手段８２、鍵暗号解読手段として鍵暗号解読手段７１、コンテンツ暗号解読手段としてコンテン

ツ暗号解読手段１４がそれぞれ該当することになる。

また、上述した第９の実施の形態では、第１鍵発生手段８０は、コンテンツ暗号化手段１３が入力したＡＶデータＤを暗号化するためのコンテンツ鍵Ｋｃｏを発生するとした。しかし、本発明の記録装置は、図２９に示すように、第１鍵発生手段８０を備えず、コンテンツ暗号化手段１３は、放送局から送られてくる放送スクランブル鍵Ｋｓを、放送デスクランブル手段２０を介して入力し、その放送スクランブル鍵Ｋｓで、または、その放送スクランブル鍵Ｋｓを加工したもので、ＡＶデータＤを暗号化するとしてもよい。その場合、鍵暗号化手段７０は、コンテンツ暗号化手段１３から、放送スクランブル鍵Ｋｓ、または、その放送スクランブル鍵Ｋｓを加工したものを入力し、それを鍵暗号化鍵Ｋｘで暗号化する。

また、上述した第９の実施の形態では、コンテンツ暗号化手段１３は、第１鍵発生手段８０からのコンテンツ鍵ＫｃｏでＡＶデータＤを暗号化するとした。しかし、本発明の記録装置は、図３０に示すように、第１鍵発生手段８０、鍵暗号化手段１５を備えず、コンテンツ暗号化手段１３は、第２鍵発生手段８１からの鍵暗号化鍵ＫｘをＫｘＦＩＦＯ８５を介して入力し、その鍵暗号化鍵Ｋｘをコンテンツ鍵Ｋｘとして使用し、そのコンテンツ鍵Ｋｘにより、ＡＶデータＤを暗号化するとしてもよい。この場合、記録媒体６には、コンテンツ鍵Ｋｘにより暗号化されたＡＶデータＤ、つまり、Ｋｘ（ＡＶデータ）と、コンテンツ鍵Ｋｘとが記録される。またその場合、本発明の再生装置は、図３０に示すように、鍵復元手段１６を備えないことになる。したがって、Ｋｘ（ＡＶデータ）を再生しようとする場合、コンテンツ鍵取得手段８３は、対応するコンテンツ鍵Ｋｘを特定し、それをＫｘＦＩＦＯ８５

のなかから取得する。そして、コンテンツ暗号解読手段１４は、記録媒体６からのＫｘ（ＡＶデータ）をＤＭＵＸ５７を介して入力するとともに、鍵暗号化鍵取得手段８２からのコンテンツ鍵ＫｘをＫｘラッチ手段８６を介して入力し、そのコンテンツ鍵ＫｘでＫｘ（ＡＶデータ）を暗号解読する。そのため、この場合、つまり、請求項５３および２０の本発明では、コンテンツ鍵発生手段として第２鍵発生手段８１、格納手段としてＫｘＦＩＦＯ８５、コンテンツ暗号化手段としてコンテンツ暗号化手段１３、対応関係情報生成手段として対応関係情報生成手段８４、記録手段としてＤＭＵＸ２３がそれぞれ該当することになる。また、請求項５７および２２の本発明では、コンテンツ鍵取得手段としてコンテンツ鍵取得手段８３、コンテンツ暗号解読手段としてコンテンツ暗号解読手段１４がそれぞれ該当することになる。

また、上述した第９の実施の形態の記録装置は、図３１に示すように、課金手段８８を備え、記録媒体６に暗号化されたＡＶデータＫｃｏ（Ｄ）を記録するさい、その記録に対する所定の課金をユーザに課し、あらかじめユーザから所定の料金が放送局等に支払われた場合、もしくは、少なくとも記録するさいに所定の料金が支払われた場合のみ、暗号化されたＡＶデータＫｃｏ（Ｄ）は記録媒体６に記録されるとしてもよい。また、課金手段８８は、図３１に示す位置に配置されなくとも、鍵暗号化手段１５とＭＵＸ５４との間に配置されるとしてもよい。要するに、課金手段８８は、記録媒体６に暗号化されたＡＶデータＫｃｏ（Ｄ）を記録するさい、その記録に対する所定の課金をユーザに課すものでありさえすればよく、配置場所はどの場所であってもよい。

また、上述した第９の実施の形態では、鍵暗号化鍵Ｋｘそれぞれは、発生

から１週間経過すると廃棄されるとしたが、廃棄される日時は、発生から１週間経過後に限定することはなく、１日経過後であっても、３日経過後であっても、または、１２時間経過後であってもよい。要するに、鍵暗号化鍵Ｋｘそれぞれは、発生から所定の期間経過すると廃棄されさえすればよい。

また、上述した第９の実施の形態では、第２鍵発生手段８１は、毎日、１つづつ異なる鍵暗号化鍵Ｋｘを発生するとしたが、第２鍵発生手段８１は、同じ日であっても、数時間毎に異なる鍵暗号化鍵Ｋｘを発生するとしてもよい。さらに、記録媒体６に所定の番組の暗号化されたＡＶデータＫｃｏ（Ｄ）を記録する毎に鍵暗号化鍵Ｋｘを発生するとしてもよい。つまり、一回の記録開始からその記録の終了毎に、その都度、鍵暗号化鍵Ｋｘを発生するとしてもよい。要するに、第２鍵発生手段８１は、記録しようとする暗号化されたＡＶデータＫｃｏ（Ｄ）のコンテンツ鍵Ｋｃｏを暗号化するための鍵暗号化鍵Ｋｘを発生しさえすればよい。

また、上述した第９の実施の形態では、本発明の対応関係情報として、鍵暗号化鍵Ｋｘが発生されたさいの日時情報を用いたが、本発明の対応関係情報は、コンテンツ暗号化手段１３がＡＶデータＤを入力した日時、コンテンツ暗号化手段１３がコンテンツ鍵ＫｃｏでＡＶデータＤをコンテンツ暗号化した日時、第２鍵発生手段８１が鍵暗号化鍵Ｋｘを発生した日時、ＫｘＦＩＦＯ８５が鍵暗号化鍵Ｋｘを格納した日時、鍵暗号化手段７０が鍵暗号化鍵Ｋｘでコンテンツ鍵Ｋｃｏを暗号化した日時、または、ＭＵＸ５４が記録媒体６に暗号化されたＡＶデータＫｃｏ（Ｄ）を記録した日時の情報であってもよい。もしくは、上述した鍵暗号化鍵Ｋｘが発生されたさいの日時や、コンテンツ暗号化手段１３がＡＶデータＤを入力した日時等と、ＡＶデータを

再生しようとする日時との情報であってもよい。その場合、図２７の鍵暗号化鍵Ｋｘリストの各鍵暗号化鍵Ｋｘが毎日順位を下げることに基づいて、また、２つの日時の差が考慮されて、鍵暗号化鍵Ｋｘが取得されることになる。または、本発明の対応関係情報は、上述した鍵暗号化鍵Ｋｘが発生されたさいの日時や、コンテンツ暗号化手段１３がＡＶデータＤを入力した日時等と、ＡＶデータを再生しようとする日時とに基づき、また、図２７の鍵暗号化鍵Ｋｘリストの各鍵暗号化鍵Ｋｘが毎日順位を下げることが考慮された、図２７の鍵暗号化鍵Ｋｘリストの番号情報等であってもよい。

また、上述した第９の実施の形態では、記録媒体としての記録媒体６を用いたが、記録媒体は、記録媒体６に限らず、ハードディスクであってもよい。

また、上述した第９の実施の形態では、第１鍵発生手段８０はＡＶデータＤを暗号化するためのコンテンツ鍵Ｋｃｏを発生するが、そのコンテンツ鍵Ｋｃｏは、簡単に解読することができないように、例えば数十秒などの短い期間で更新されるとしてもよい。

さらに、上述した記録装置または再生装置は、鍵暗号化鍵Ｋｘの発生から例えば１週間という所定の期間を経過するなどして、その鍵暗号化鍵Ｋｘが廃棄されたり、使用不可になる前に、その鍵暗号化鍵Ｋｘに対応する暗号化されたＡＶデータＫｃｏ（Ｄ）が一度も再生されていない場合、その旨の情報をユーザに通知する手段を備えてもよい。

産業上の利用可能性

以上説明したところから明らかなように、請求項１の本発明は、データに暗号化を施すことによって、特定の対象に対してのみ、再生が可能であり、

前記暗号化に関する情報が外部に漏洩しにくいデータ記録再生方法を提供することができる。また、請求項４の本発明は、データに暗号化を施すことによって、特定の対象に対してのみ、再生が可能であり、前記暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムを提供することができる。また、請求項２２または２３の本発明は、記録および／または再生時に、確実に課金が可能なデータ記録再生方法およびデータ記録再生システムを提供することができる。さらに、請求項３０の本発明は、再生時のロスタイムが少ないデータ記録再生システムを提供することができる。

さらに、本発明は、ＡＶデータを記録媒体に記録し、そのＡＶデータの有効再生期間や有効再生回数の制限を遵守する記録装置および再生装置を提供することができる。

なお、本発明のプログラム媒体は、上述した発明の各構成要素の全部又は一部をコンピュータで実現するためのプログラムを格納したことを特徴とするＣＤ－ＲＯＭ等のプログラム媒体である。

請　求　の　範　囲

1．　ディジタルデータにコンテンツ鍵を用いて第１の暗号化を施した暗号化ディジタルデータと、前記コンテンツ鍵に第２の暗号化を施した暗号化コンテンツ鍵とを記録媒体に記録し、記録された前記暗号化ディジタルデータおよび前記暗号化コンテンツ鍵を再生し、前記暗号化コンテンツ鍵を解読して得られた前記コンテンツ鍵を用いて前記暗号化ディジタルデータを解読して、前記ディジタルデータを得ることを特徴とするデータ記録再生方法。

2．　前記暗号化コンテンツ鍵を、前記記録媒体の外部に出力されないデータ領域に記録することを特徴とする請求項１に記載のデータ記録再生方法。

3．　前記コンテンツ鍵を、定期的または不定期的に切り替えることを特徴とする請求項１または２に記載のデータ記録再生方法。

4．　ディジタルデータを入力するとともに、前記ディジタルデータを暗号化するためのコンテンツ鍵を入力し、そのコンテンツ鍵を用いて前記ディジタルデータに第１の暗号化を施して暗号化ディジタルデータを生成するコンテンツ暗号化手段と、前記コンテンツ鍵に第２の暗号化を施して暗号化コンテンツ鍵を生成する鍵暗号化手段と、前記暗号化ディジタルデータおよび前記暗号化コンテンツ鍵を記録媒体に記録する記録手段と、前記記録媒体から前記暗号化ディジタルデータおよび前記暗号化コンテンツ鍵を再生する再生手段と、前記暗号化コンテンツ鍵を解読して前記コンテンツ鍵を復元する鍵暗号解読手段と、復元された前記コンテンツ鍵を用いて前記暗号化ディジタルデータを解読して、前記ディジタルデータを得るコンテンツ暗号解読手段とを備えることを特徴とするデータ記録再生システム。

5．　前記全ての手段は、一体化された装置に備えられていることを特徴

とする請求項４に記載のデータ記録再生システム。

６．　前記受信手段と、前記コンテンツ暗号化手段と、前記コンテンツ暗号解読手段とは、チューナ装置に備えられ、前記記録手段と、前記再生手段とは、ＶＴＲ装置に備えられていることを特徴とする請求項４に記載のデータ記録再生システム。

７．　前記第２の暗号化は、公開鍵を用いて施され、前記暗号化コンテンツ鍵の解読は、前記公開鍵に対応する秘密鍵を用いて施されることを特徴とする請求項６に記載のデータ記録再生システム。

８．　前記鍵暗号解読手段は、前記チューナ装置に備えられていることを特徴とする請求項７に記載のデータ記録再生システム。

９．　前記公開鍵および前記秘密鍵は、前記チューナ装置に対して固有な鍵であることを特徴とする請求項８に記載のデータ記録再生システム。

１０．　前記公開鍵および前記秘密鍵は、前記チューナ装置の機器モデルに対して固有な鍵であることを特徴とする請求項８に記載のデータ記録再生システム。

１１．　前記チューナ装置は、ＩＣカードに記録された情報を読み取るカード読取手段を有することを特徴とする請求項８に記載のデータ記録再生システム。

１２．　前記公開鍵および前記秘密鍵は、前記ＩＣカードに記録されたユーザＩＤに対して固有な鍵であることを特徴とする請求項１１に記載のデータ記録再生システム。

１３．　前記公開鍵および前記秘密鍵は、前記ＩＣカードに記録されたサービスに対して固有な鍵であることを特徴とする請求項１１に記載のデータ

記録再生システム。

１４．　前記ＩＣカードには、前記ユーザＩＤに対して固有な鍵に加えて、少なくとも一つの別のユーザＩＤに対して固有な公開鍵が記録されており、前記鍵暗号化手段は、前記第２の暗号化とともに、前記別のユーザＩＤに対して固有な公開鍵を用いて、前記コンテンツ鍵を暗号化して、前記別のユーザＩＤに対して固有な公開鍵毎に、別の暗号化コンテンツ鍵を生成し、前記記録手段は、前記暗号化コンテンツ鍵に加えて、前記別の暗号化コンテンツ鍵も前記記録媒体に記録することを特徴とする請求項１２に記載のデータ記録再生システム。

１５．　前記鍵暗号化手段は、前記チューナ装置または前記ＶＴＲ装置のいずれかに備えられていることを特徴とする請求項８～１４のいずれかに記載のデータ記録再生システム。

１６．　前記鍵暗号化手段が前記ＶＴＲ装置に備えられている場合は、前記チューナ装置は、前記コンテンツ鍵を共通鍵によって暗号化する第二の鍵暗号化手段を有し、前記ＶＴＲ装置は、前記共通鍵によって暗号化された前記コンテンツ鍵を解読する第二の鍵暗号解読手段を有することを特徴とする請求項１５に記載のデータ記録再生システム。

１７．　前記公開鍵および前記秘密鍵は、前記ＶＴＲ装置に対して固有な鍵であり、前記鍵暗号化手段および前記鍵暗号解読手段は、前記ＶＴＲ装置に備えられていることを特徴とする請求項７に記載のデータ記録再生システム。

１８．　前記チューナ装置は、前記コンテンツ鍵を共通鍵によって暗号化する第二の鍵暗号化手段と、前記共通鍵によって暗号化された前記コンテン

ツ鍵を解読する第二の鍵暗号解読手段とを有し、前記ＶＴＲ装置は、前記コンテンツ鍵を前記共通鍵によって暗号化する第三の鍵暗号化手段と、前記共通鍵によって暗号化された前記コンテンツ鍵を解読する第三の鍵暗号解読手段とを有し、前記第三の鍵暗号解読手段は、前記第二の鍵暗号化手段により暗号化された前記コンテンツ鍵を解読し、前記第二の鍵暗号解読手段は、前記第三の鍵暗号化手段により暗号化された前記コンテンツ鍵を解読することを特徴とする請求項１７に記載のデータ記録再生システム。

１９．　前記第２の暗号化および前記暗号化コンテンツ鍵の解読は、共通鍵を用いて施され、前記鍵暗号化手段および前記鍵暗号解読手段は、前記チューナ装置に備えられていることを特徴とする請求項６に記載のデータ記録再生システム。

２０．　前記共通鍵は、前記チューナ装置、もしくは、前記チューナ装置の機器モデルに対して固有な鍵であることを特徴とする請求項１９に記載のデータ記録再生システム。

２１．　前記チューナ装置は、ＩＣカードに記録された情報を読み取るカード読取手段を有し、前記共通鍵は、前記ＩＣカードに記録されたユーザＩＤ、もしくは、前記ＩＣカードに記録されたサービスに対して固有な鍵に対して固有な鍵であることを特徴とする請求項１９に記載のデータ記録再生システム。

２２．　前記チューナ装置は、前記記録媒体の記録時に課金情報を生成し、それを記憶することを特徴とする請求項６～２１のいずれかに記載のデータ記録再生システム。

２３．　前記チューナ装置は、前記記録媒体の再生時に課金情報を生成し

、それを記憶することを特徴とする請求項６～２１のいずれかに記載のデータ記録再生システム。

２４．　前記記録媒体の記録時に、前記課金情報を生成するために必要な情報を、前記記録媒体に記録し、前記記録媒体の再生時に前記必要な情報を用いて前記課金情報を生成することを特徴とする請求項２３に記載のデータ記録再生システム。

２５．　前記課金情報は、前記記録媒体の再生期間の限定を伴うものであることを特徴とする請求項２３または２４に記載のデータ記録再生システム。

２６．　前記課金情報は、前記記録媒体の再生回数の限定を伴うものであることを特徴とする請求項２３～２５のいずれかに記載のデータ記録再生システム。

２７．　前記チューナ装置は、前記ＩＣカードに前記課金情報を記憶させることを特徴とする請求項２２～２６のいずれかに記載のデータ記録再生システム。

２８．　前記チューナ装置は、前記課金情報をサービスプロバイダに対して、通信を介して、出力することを特徴とする請求項２２～２７のいずれかに記載のデータ記録再生システム。

２９．　前記暗号化コンテンツ鍵を、前記記録媒体の外部に出力されないデータ領域に記録することを特徴とする請求項４～２８のいずれかに記載のデータ記録再生システム。

３０．　前記第２の暗号化を施した鍵の固有性に関する情報を、前記記録媒体に記録することを特徴とする請求項４～２９のいずれかに記載のデータ記録再生システム。

３１．　前記コンテンツ鍵を、定期的または不定期的に切り替えることを特徴とする請求項４～３０のいずれかに記載のデータ記録再生システム。

３２．　前記切り替えの後のコンテンツ鍵に対応する前記暗号化コンテンツ鍵が、前記切り替えの前のコンテンツ鍵に対応する前記暗号化ディジタルデータの少なくとも一部とタイミング的に重なるように、前記記録媒体は再生されることを特徴とする請求項３１に記載のデータ記録再生システム。

３３．　一つの前記コンテンツ鍵に対応する前記暗号化コンテンツ鍵が、それに対応する前記暗号化ディジタルデータとタイミング的に重なるように、前記記録媒体は再生されることを特徴とする請求項３１または３２に記載のデータ記録再生システム。

３４．　前記チューナ装置を備える場合は、前記チューナ装置が前記切り替えを行うことを特徴とする請求項３１～３３のいずれかに記載のデータ記録再生システム。

３５．　前記ＶＴＲ装置を備える場合は、前記ＶＴＲ装置が、前記切り替えに対応して、前記暗号化コンテンツ鍵の再生のタイミングを決定することを特徴とする請求項３１～３４のいずれかに記載のデータ記録再生システム。

３６．　前記暗号化ディジタルデータおよび前記暗号化コンテンツ鍵は、前記記録媒体上の前記再生のタイミングに対応する記録位置に、記録されることを特徴とする請求項３１～３５のいずれかに記載のデータ記録再生システム。

３７．　前記切り替えのタイミングも合わせて、前記記録媒体に記録することを特徴とする請求項３６に記載のデータ記録再生システム。

３８．　前記チューナ装置および前記ＶＴＲ装置を備える場合は、前記Ｖ

ＴＲ装置が、前記切り替えの後のコンテンツ鍵、もしくは、それに対応する前記暗号化コンテンツ鍵を、前記切り替えの後のコンテンツ鍵に対応する前記暗号化ディジタルデータの出力より前もって、前記チューナ装置へ出力することを特徴とする請求項３１～３７のいずれかに記載のデータ記録再生システム。

３９．ディジタルデータを入力するとともに、前記ディジタルデータを暗号化するためのコンテンツ鍵を入力し、そのコンテンツ鍵を用いて前記ディジタルデータに第１の暗号化を施して暗号化ディジタルデータを生成するコンテンツ暗号化手段と、

前記コンテンツ鍵に第２の暗号化を施すための鍵暗号化鍵を発生する鍵暗号化鍵発生手段と、前記鍵暗号化鍵を格納し、その後、その鍵暗号化鍵が所定の条件に合えば、その鍵暗号化鍵を消去する格納手段と、

前記鍵暗号化鍵で前記コンテンツ鍵に第２の暗号化を施して暗号化コンテンツ鍵を生成する鍵暗号化手段と、

前記コンテンツ鍵により暗号化した暗号化ディジタルデータと、そのコンテンツ鍵を暗号化した鍵暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、

前記暗号化ディジタルデータ、前記暗号化コンテンツ鍵、および、前記対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを

備えたことを特徴とする記録装置。

４０．前記所定の条件とは、前記鍵暗号化鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項３９記載の記録装置。

４１．前記対応関係情報とは、前記コンテンツ暗号化手段が前記ディジタルデータを入力した日時、前記コンテンツ暗号化手段が前記コンテンツ鍵で前記ディジタルデータを暗号化した日時、前記鍵暗号化鍵発生手段が前記鍵暗号化鍵を発生した日時、前記格納手段が前記鍵暗号化鍵を格納した日時、前記鍵暗号化手段が前記鍵暗号化鍵で前記コンテンツ鍵を暗号化した日時、または、前記記録手段が前記所定の記録媒体に前記暗号化ディジタルデータを記録した日時で対応付けられた情報であることを特徴とする請求項３９または４０記載の記録装置。

４２．前記所定の条件とは、前記暗号化ディジタルデータの再生のさいに、前記鍵暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項３９記載の記録装置。

４３．前記コンテンツ鍵を発生するコンテンツ鍵発生手段を備え、前記コンテンツ暗号化手段は、前記コンテンツ鍵発生手段から前記コンテンツ鍵を入力することを特徴とする請求項３９から４２のいずれかに記載の記録装置。

４４．前記コンテンツ暗号化手段は、放送局からの前記コンテンツ鍵を入力し、そのコンテンツ鍵を利用することを特徴とする請求項３９から４２のいずれかに記載の記録装置。

４５．請求項３９から４４のいずれかに記載の記録装置における前記記録媒体上の前記対応関係情報を入力し、その対応関係情報に基づいて、再生しようとする暗号化ディジタルデータに対応する鍵暗号化鍵を特定し、前記記録装置における前記格納手段のなかの前記鍵暗号化鍵を検索して取得する鍵暗号化鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとする暗号化ディジタルデー

タに対応する、暗号化されたコンテンツ鍵を入力するとともに、前記鍵暗号化鍵を入力し、その鍵暗号化鍵で前記暗号化されたコンテンツ鍵の暗号化を解く鍵暗号解読手段と、

前記鍵暗号解読手段からのコンテンツ鍵で前記暗号化ディジタルデータの暗号化を解読するコンテンツ暗号解読手段とを

備えたことを特徴とする再生装置。

４６．ディジタルデータを入力するとともに、前記ディジタルデータを暗号化するためのコンテンツ鍵を入力し、そのコンテンツ鍵で前記ディジタルデータに第１の暗号化を施し暗号化ディジタルデータを生成するコンテンツ暗号化手段と、

前記コンテンツ鍵に第２の暗号化を施すための鍵暗号化鍵を発生する鍵暗号化鍵発生手段と、

前記鍵暗号化鍵発生手段が発生した鍵暗号化鍵を格納する格納手段と、

前記鍵暗号化鍵で前記コンテンツ鍵を暗号化する鍵暗号化手段と、

前記コンテンツ鍵により暗号化された暗号化ディジタルデータと、そのコンテンツ鍵を暗号化した鍵暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、

前記暗号化ディジタルデータ、前記暗号化コンテンツ鍵、および、前記対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを

備えたことを特徴とする記録装置。

４７．前記対応関係情報とは、前記コンテンツ暗号化手段が前記ディジタルデータを入力した日時、前記コンテンツ暗号化手段が前記コンテンツ鍵で

前記ディジタルデータを暗号化した日時、前記鍵暗号化鍵発生手段が前記鍵暗号化鍵を発生した日時、前記格納手段が前記鍵暗号化鍵を格納した日時、前記鍵暗号化手段が前記鍵暗号化鍵で前記コンテンツ鍵を暗号化した日時、または、前記記録手段が前記所定の記録媒体に前記暗号化ディジタルデータを記録した日時で対応付けられた情報であることを特徴とする請求項４６記載の記録装置。

４８．前記コンテンツ鍵を発生するコンテンツ鍵発生手段を備え、前記コンテンツ暗号化手段は、前記コンテンツ鍵発生手段から前記コンテンツ鍵を入力することを特徴とする請求項４６または４７記載の記録装置。

４９．前記コンテンツ暗号化手段は、放送局からの前記コンテンツ鍵を入力し、そのコンテンツ鍵を利用することを特徴とする請求項４６または４７記載の記録装置。

５０．請求項４６から４９のいずれかに記載の記録装置における前記記録媒体上の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとする暗号化ディジタルデータに対応する鍵暗号化鍵を特定し、さらに、その鍵暗号化鍵が所定の条件に合うかどうかを判定し、合致する場合は、その鍵暗号化鍵を、前記記録装置における前記格納手段から取り出し、合致しない場合は、その鍵暗号化鍵を前記格納手段から取り出さない鍵暗号化鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとする暗号化ディジタルデータに対応する、暗号化されたコンテンツ鍵を入力するとともに、前記鍵暗号化鍵を入力し、その鍵暗号化鍵で前記暗号化されたコンテンツ鍵の暗号化を解いてコンテンツ鍵を復元する鍵暗号解読手段と、

前記鍵暗号解読手段からのコンテンツ鍵で前記暗号化ディジタルデータの暗号化を解読するコンテンツ暗号解読手段とを

備えたことを特徴とする再生装置。

５１．前記所定の条件とは、請求項４６から４９のいずれかに記載の記録装置の前記格納手段に、前記鍵暗号化鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項５０記載の再生装置。

５２．前記所定の条件とは、前記暗号化ディジタルデータの再生のさいに、前記鍵暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項５０記載の再生装置。

５３．ディジタルデータを暗号化するためのコンテンツ鍵を発生するコンテンツ鍵発生手段と、

前記コンテンツ鍵発生手段が発生したコンテンツ鍵を格納し、その後、そのコンテンツ鍵が所定の条件に合えば、そのコンテンツ鍵を消去する格納手段と、

前記コンテンツ鍵で前記ディジタルデータを暗号化するコンテンツ暗号化手段と、

前記コンテンツ鍵により暗号化された暗号化ディジタルデータと、そのコンテンツ鍵との対応関係情報を生成する対応関係情報生成手段と、前記暗号化ディジタルデータ、および、前記対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを

備えたことを特徴とする記録装置。

５４．前記所定の条件とは、前記コンテンツ鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項５３記載の記録装置。

５５．前記対応関係情報とは、前記コンテンツ暗号化手段が前記ディジタルデータを入力した日時、前記コンテンツ暗号化手段が前記コンテンツ鍵で前記ディジタルデータを暗号化した日時、前記コンテンツ鍵発生手段が前記コンテンツ鍵を発生した日時、前記格納手段が前記コンテンツ鍵を格納した日時、または、前記記録手段が前記所定の記録媒体に前記暗号化ディジタルデータを記録した日時で対応付けられた情報であることを特徴とする請求項５３または５４記載の記録装置。

５６．前記所定の条件とは、前記暗号化ディジタルデータの再生のさいに、前記鍵暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項５３記載の記録装置。

５７．請求項５３から５６のいずれかに記載の記録装置の前記記録媒体上の前記対応関係情報を入力し、その対応関係情報に基づいて、再生しようとする暗号化ディジタルデータに対応するコンテンツ鍵を特定し、前記記録装置の前記格納手段のなかの前記コンテンツ鍵を検索して取得するコンテンツ鍵取得手段と、

前記所定の記録媒体から前記暗号化ディジタルデータを入力するとともに、前記コンテンツ鍵を入力し、そのコンテンツ鍵で前記暗号化ディジタルデータの暗号化を解読するコンテンツ暗号解読手段とを

備えたことを特徴とする再生装置。

５８．ディジタルデータを暗号化するためのコンテンツ鍵を発生するコンテンツ鍵発生手段と、

前記コンテンツ鍵発生手段が発生したコンテンツ鍵を格納する格納手段と

前記コンテンツ鍵で前記ディジタルデータを暗号化して暗号化ディジタルデータを得るコンテンツ暗号化手段と、

前記コンテンツ鍵により暗号化された暗号化ディジタルデータと、そのコンテンツ鍵との対応関係情報を生成する対応関係情報生成手段と、前記暗号化ディジタルデータ、および、前記対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを

備えたことを特徴とする記録装置。

５９．前記対応関係情報とは、前記コンテンツ暗号化手段が前記ディジタルデータを入力した日時、前記コンテンツ暗号化手段が前記コンテンツ鍵で前記ディジタルデータをコンテンツ暗号化した日時、前記コンテンツ鍵発生手段が前記コンテンツ鍵を発生した日時、前記格納手段が前記コンテンツ鍵を格納した日時、または、前記記録手段が前記所定の記録媒体に前記暗号化ディジタルデータを記録した日時で対応付けられた情報であることを特徴とする請求項５８記載の記録装置。

６０．請求項５８または５９記載の記録装置の前記記録媒体上の前記対応関係情報を入力し、その対応関係情報に基づいて、再生しようとする暗号化ディジタルデータに対応するコンテンツ鍵を特定し、さらに、そのコンテンツ鍵が所定の条件に合うかどうかを判定し、合致する場合は、そのコンテンツ鍵を、前記記録装置の前記格納手段から取り出し、合致しない場合は、そのコンテンツ鍵を前記格納手段から取り出さないコンテンツ鍵取得手段と、

前記コンテンツ鍵で前記暗号化ディジタルデータの暗号化を解読するコンテンツ暗号解読手段とを

備えたことを特徴とする再生装置。

６１．前記所定の条件とは、請求項５８または５９記載の記録装置の前記格納手段に、前記コンテンツ鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項６０記載の再生装置。

６２．前記所定の条件とは、前記暗号化ディジタルデータの再生のさいに、前記コンテンツ鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項６０記載の再生装置。

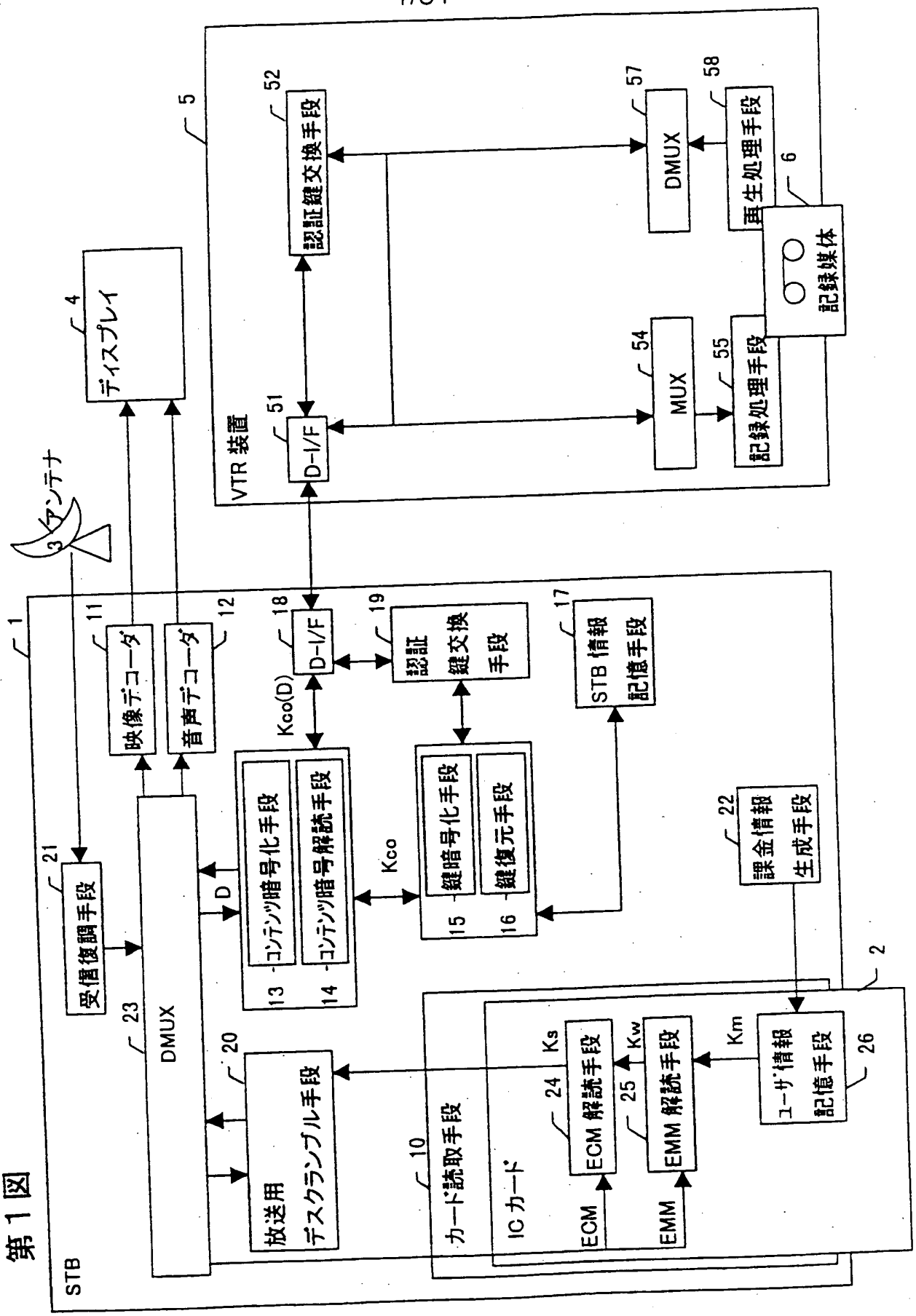
６３．前記記録手段が前記暗号化ディジタルデータを、前記所定の記録媒体に記録するさい、前記データの記録に対する課金を課す課金手段を備えたことを特徴とする請求項３９から４４のいずれか、または、請求項４６から４９のいずれか、または、請求項５３から５６のいずれか、または、請求項５８から５９のいずれかに記載の記録装置。

６４．前記所定の記録媒体は、ビデオテープであることを特徴とする請求項３９から４４のいずれか、または、請求項４６から４９のいずれか、または、請求項５３から５６のいずれか、または、請求項５８から５９のいずれかに記載の記録装置。

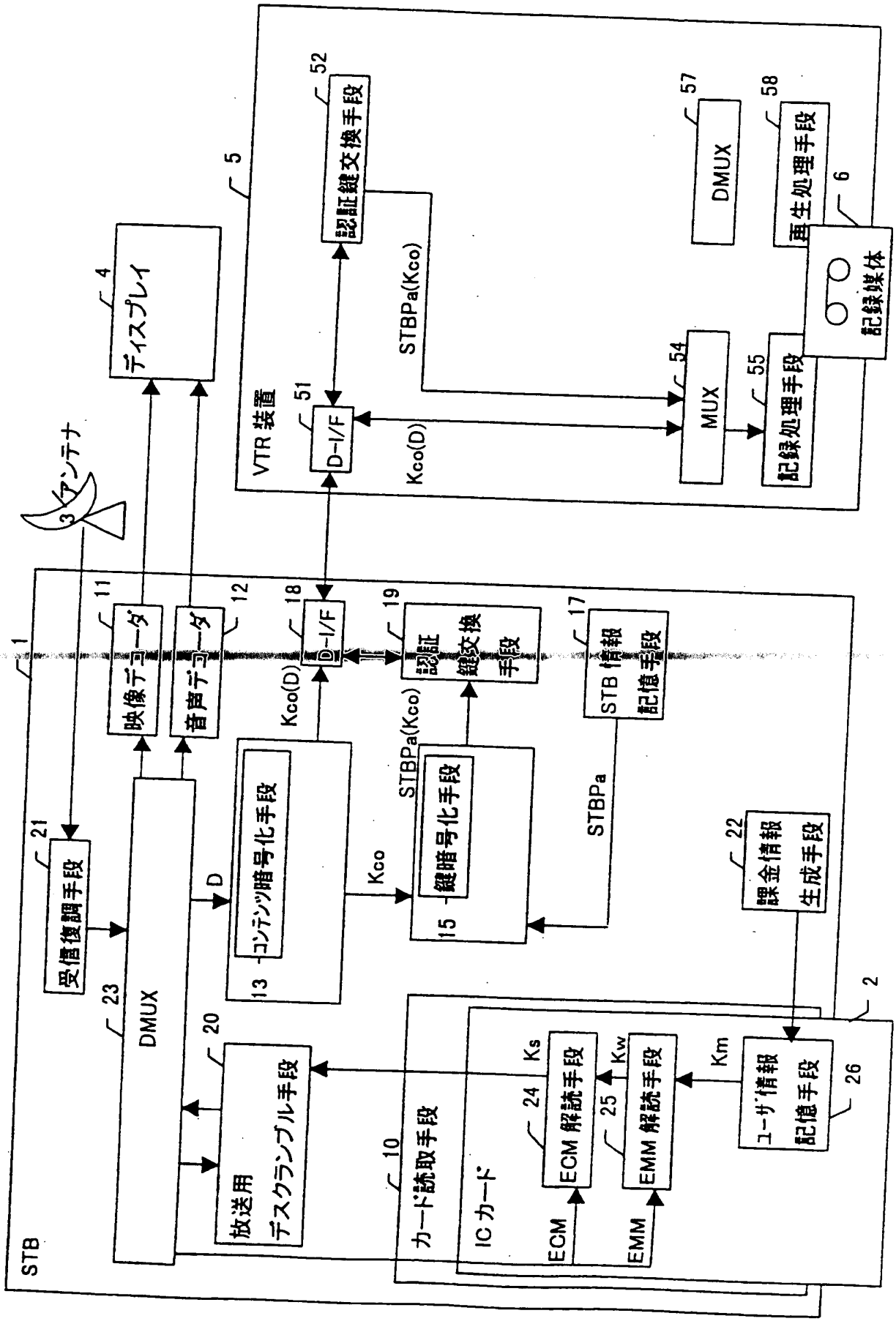
６５．前記所定の記録媒体は、ハードディスクであることを特徴とする請求項３９から４４のいずれか、または、請求項４６から４９のいずれか、または、請求項５３から５６のいずれか、または、請求項５８から５９のいずれかに記載の記録装置。

６６．請求項１～６５のいずれかに記載の請求項における各構成要素の全部又は一部をコンピュータで実現するためのプログラムを格納したことを特徴とするプログラム媒体。

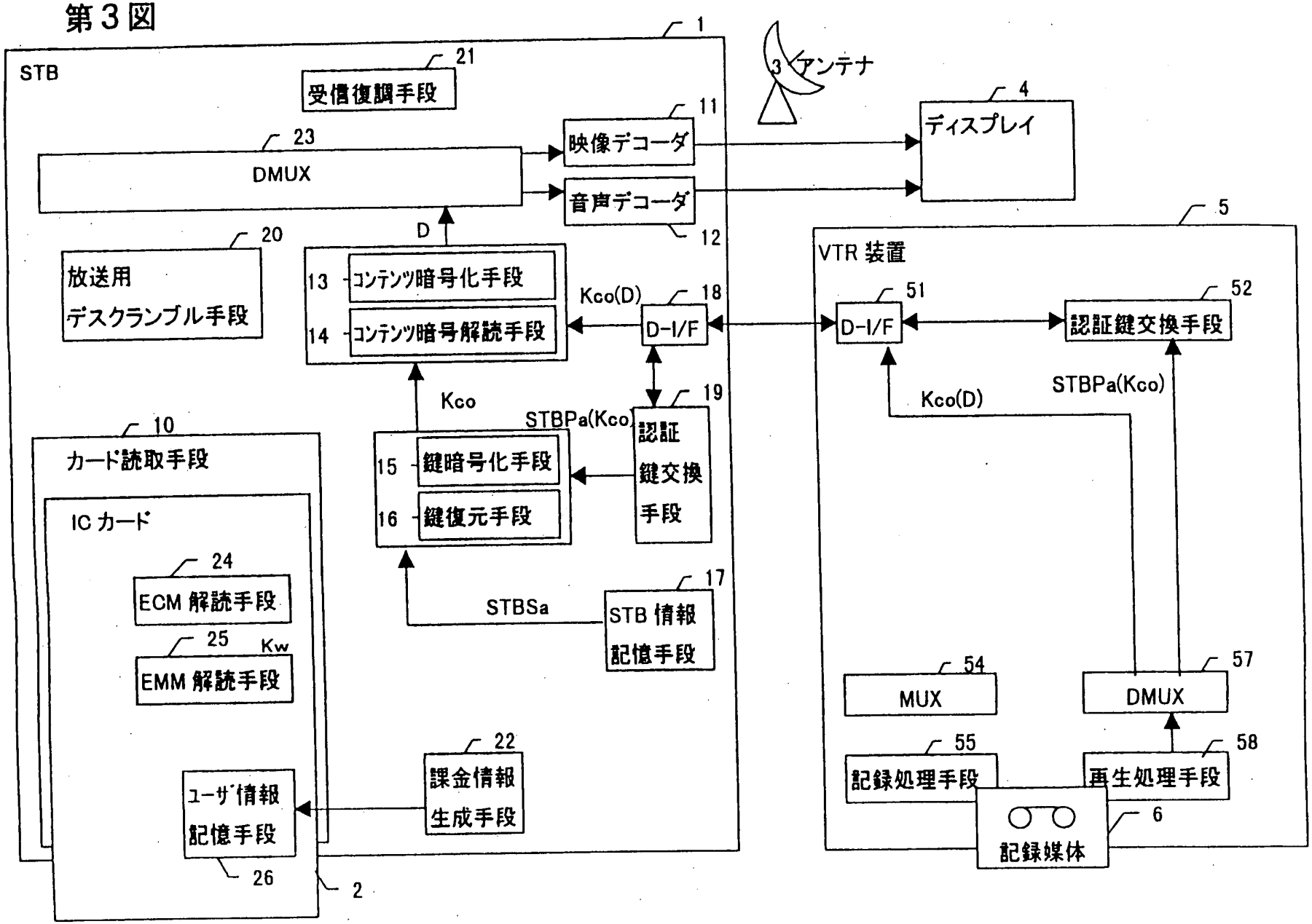
第1図


STB
1
アンテナ
3
ディスプレイ
4
VTR 装置
5
認証鍵交換手段
52
D-I/F
51
DMUX
57
再生処理手段
58
記録媒体
6
MUX
54
記録処理手段
55
映像デコーダ
11
音声デコーダ
12
D-I/F
18
認証鍵交換手段
19
STB 情報記憶手段
17
Kco(D)
コンテンツ暗号化手段
13
コンテンツ暗号解読手段
14
Kco
鍵暗号化手段
15
鍵復元手段
16
受信復調手段
21
DMUX
23
D
課金情報生成手段
22
放送用デスクランブル手段
20
カード読取手段
10
2
IC カード
Ks
ECM 解読手段
24
Kw
EMM 解読手段
25
Km
ユーザ情報記憶手段
26
ECM
EMM

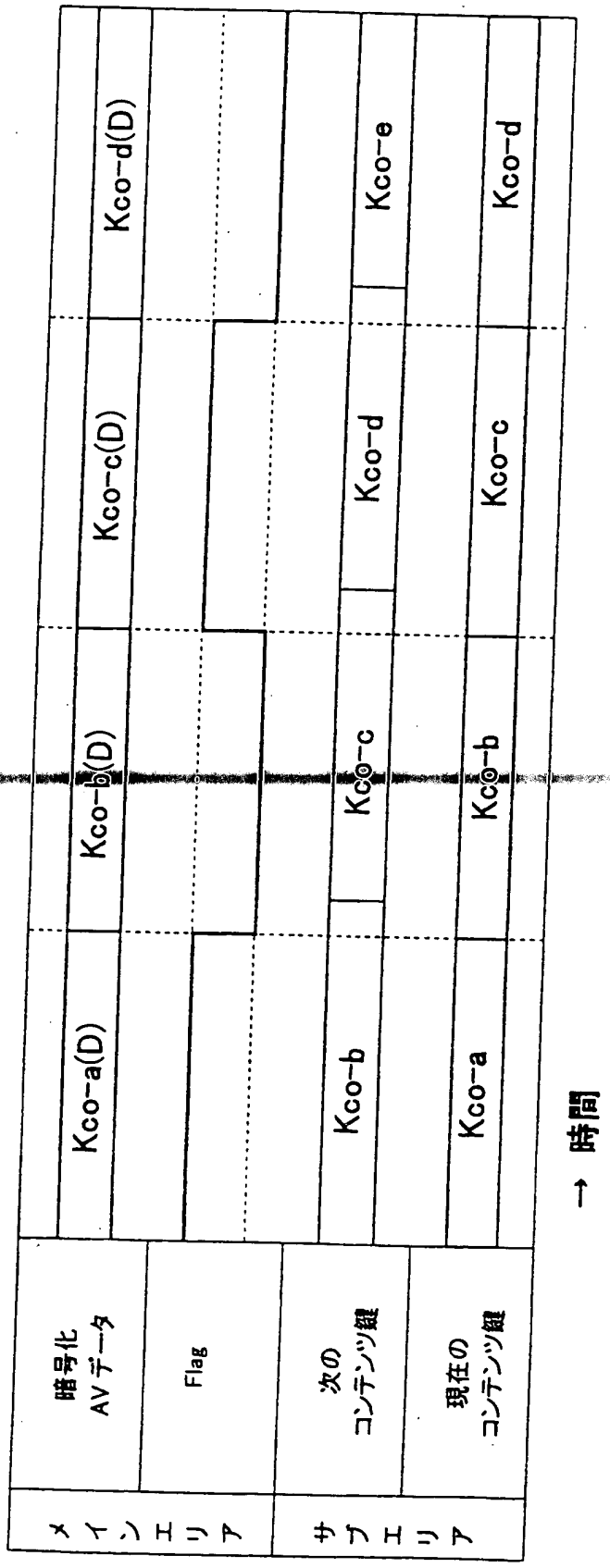
第2図

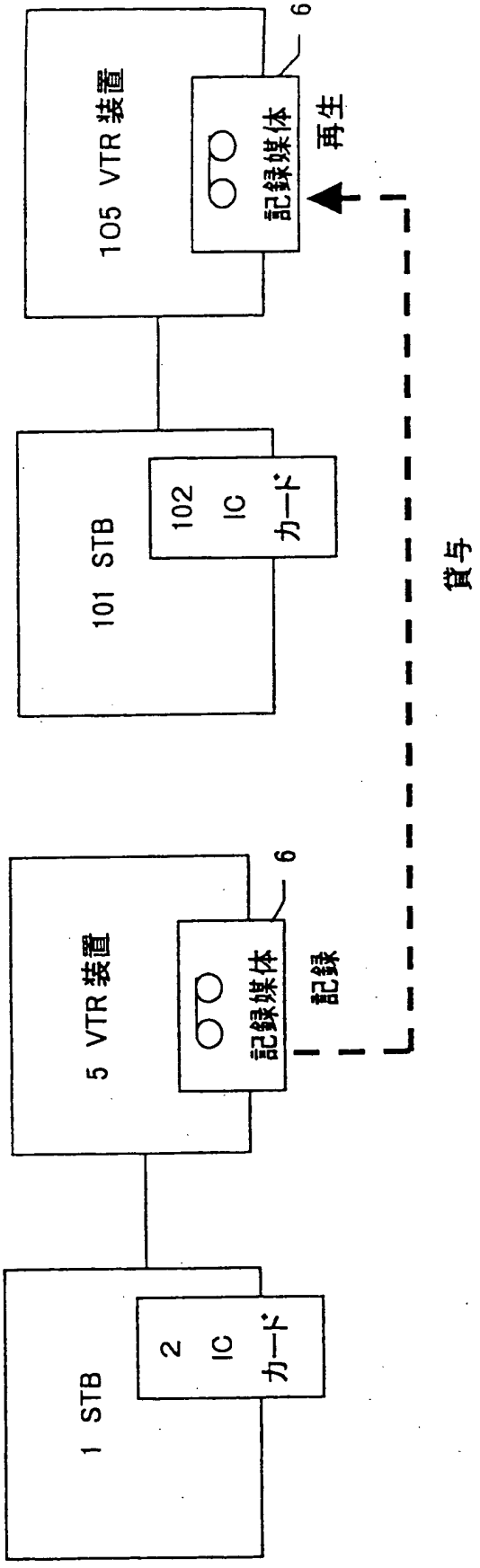


第３図



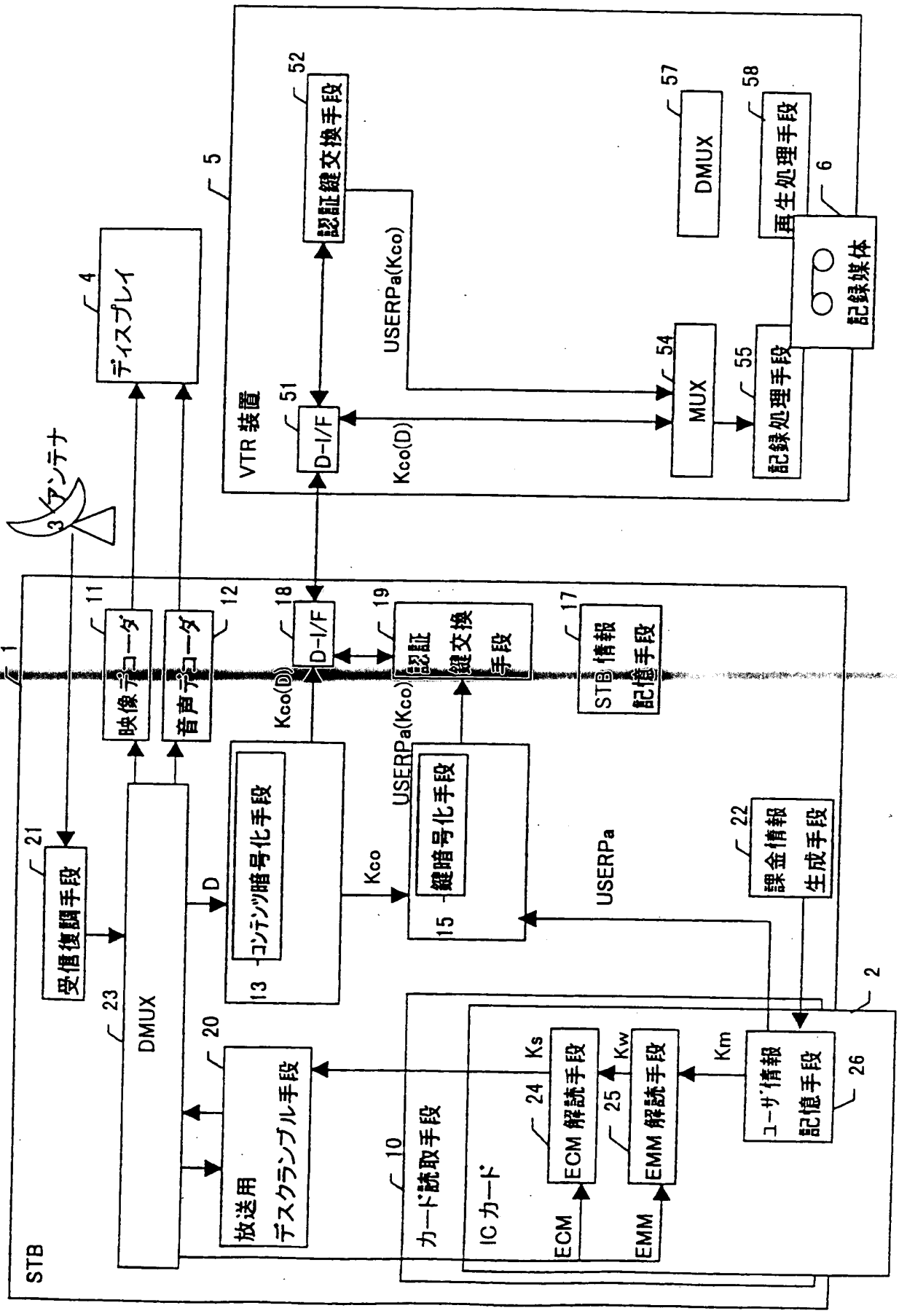
第4図



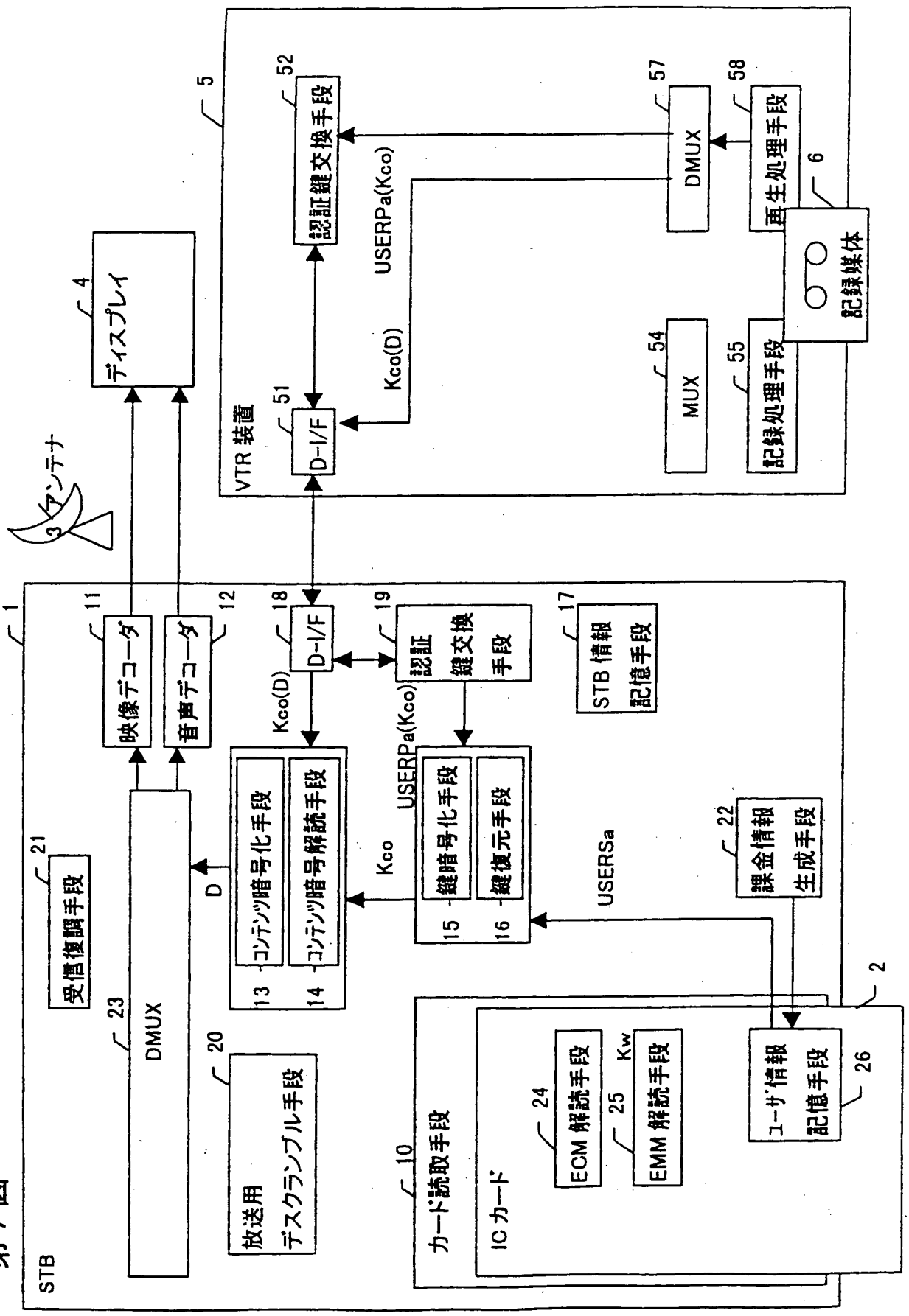

1 STB
2 IC カード
5 VTR 装置
6 記録媒体
記録
101 STB
102 IC カード
105 VTR 装置
6 記録媒体
再生
貸与

第5図

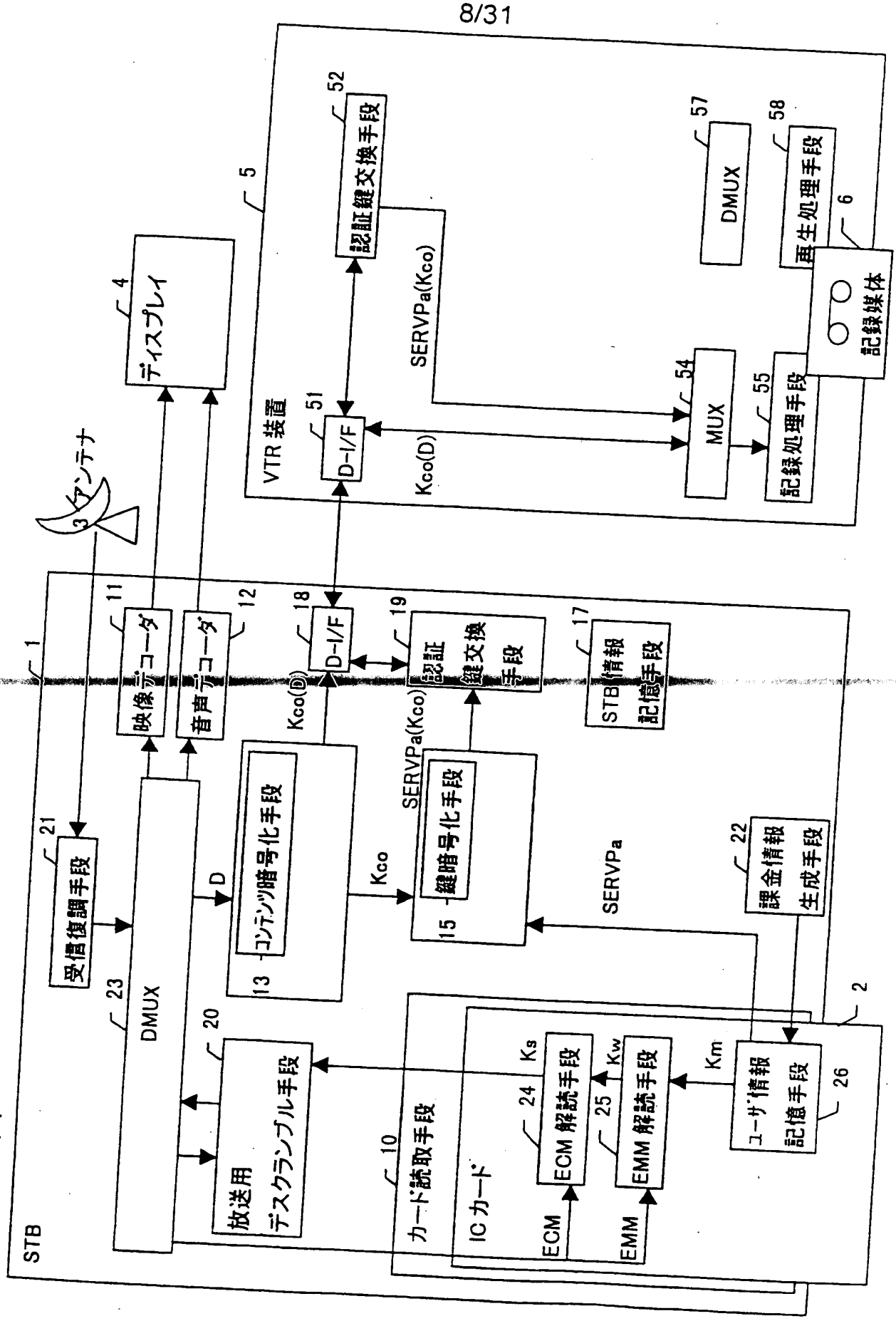
第6図



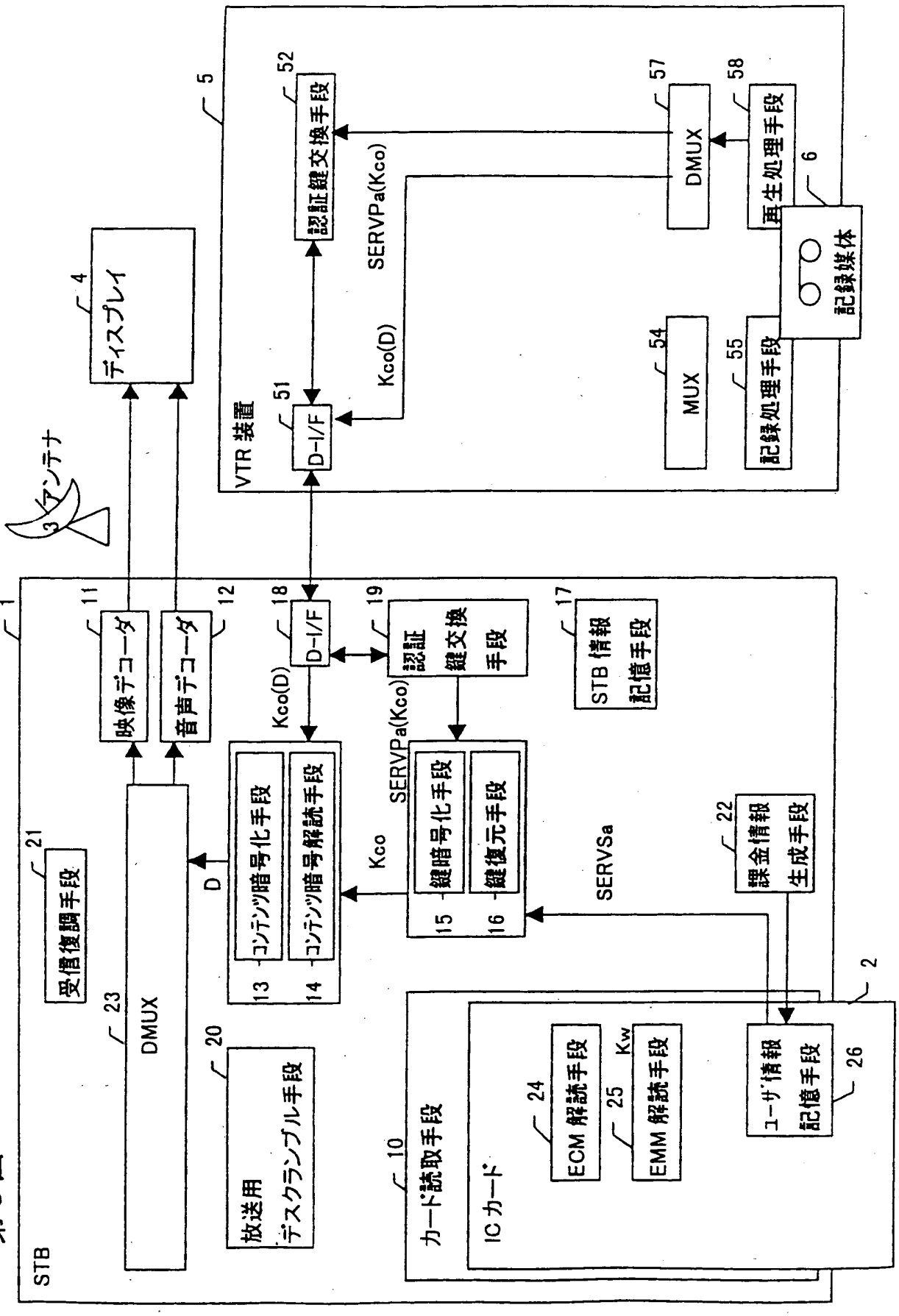
第7図



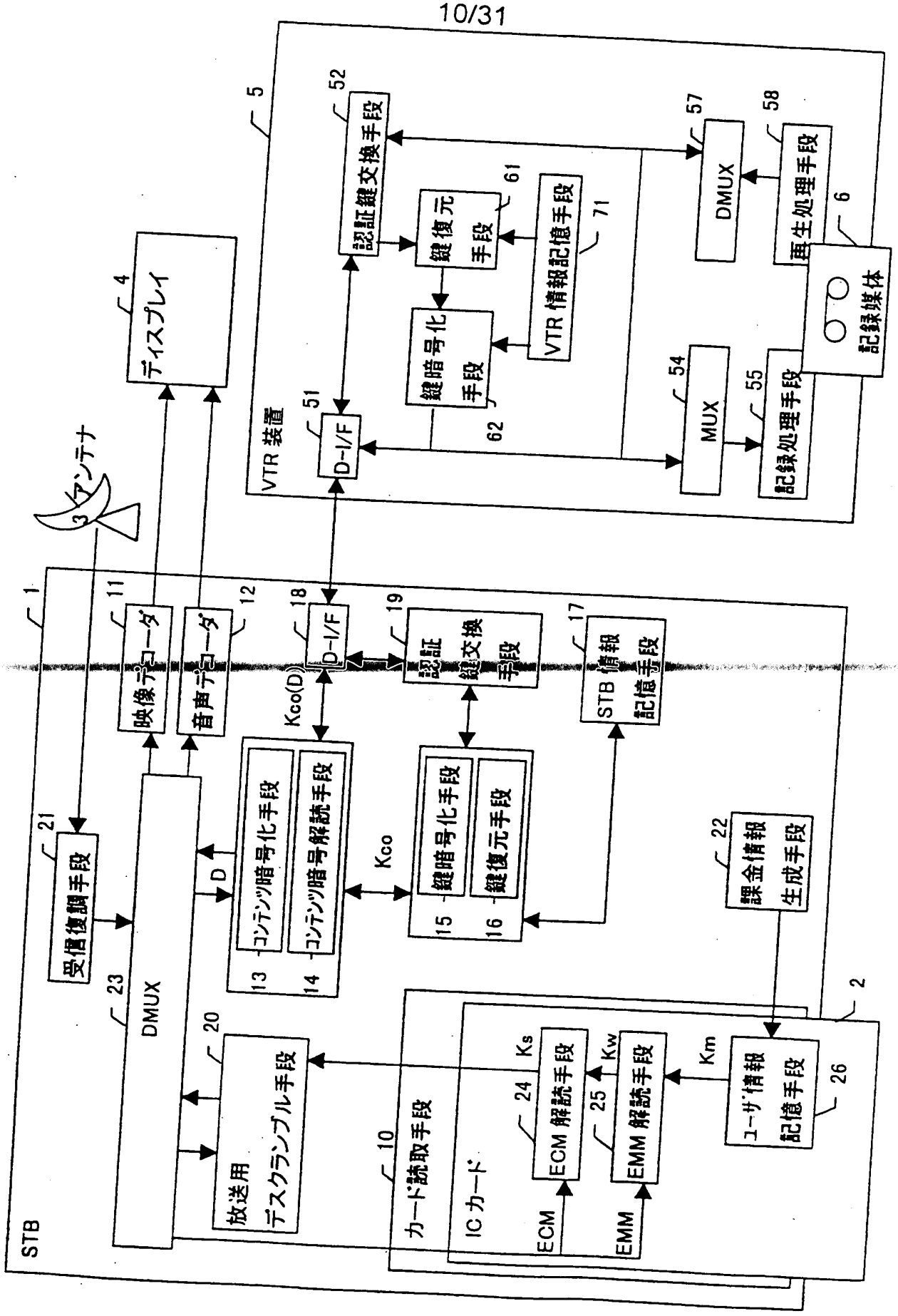
第8図



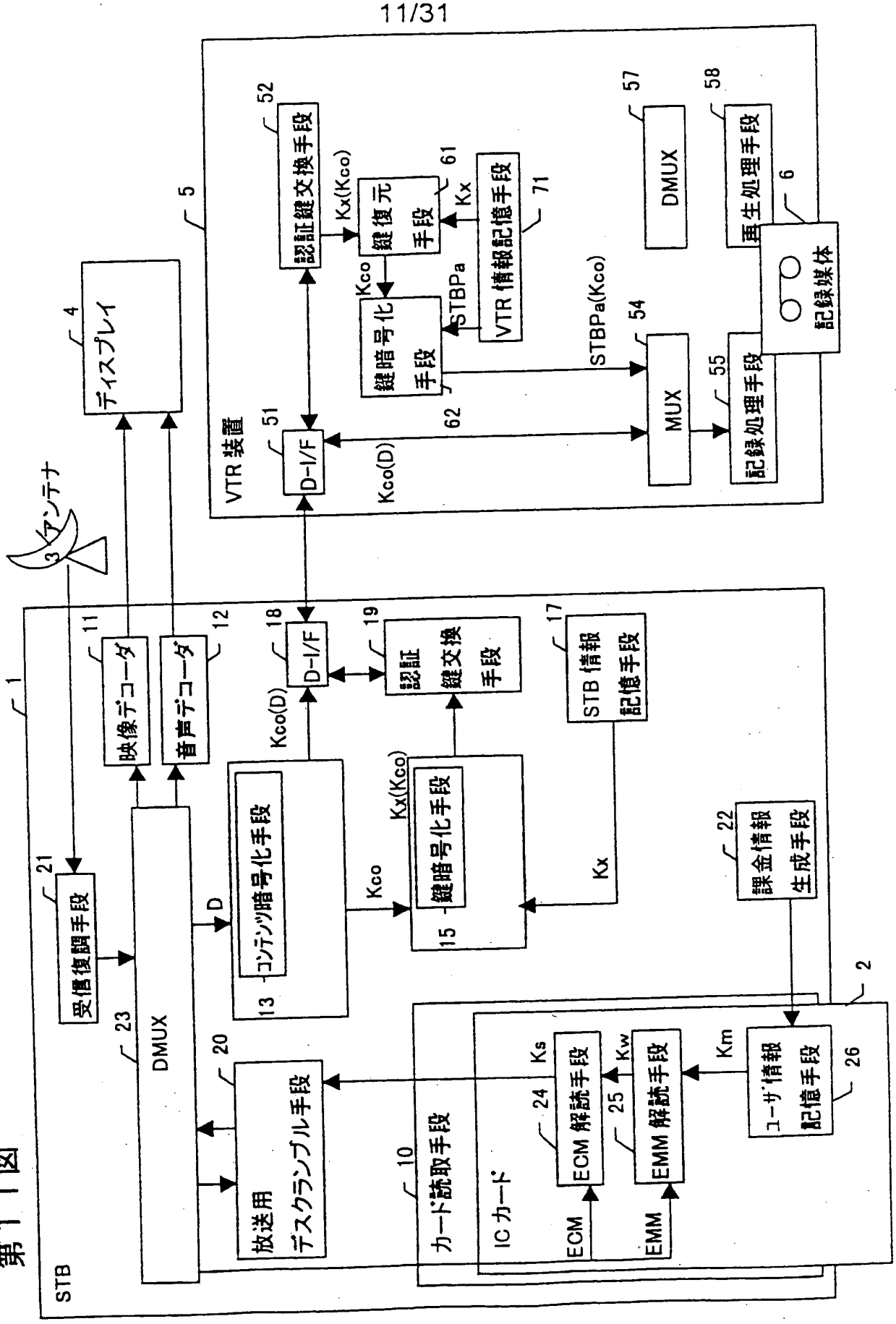
第9図


STB
1
アンテナ
3
ディスプレイ
4
VTR 装置
5
再生処理手段
6
記録媒体
2
映像デコーダ
11
音声デコーダ
12
D-I/F
18
認証鍵交換手段
19
STB 情報記憶手段
17
受信復調手段
21
DMUX
23
放送用デスクランブル手段
20
コンテンツ暗号化手段
13
コンテンツ暗号解読手段
14
鍵暗号化手段
15
鍵復元手段
16
課金情報生成手段
22
カード読取手段
10
IC カード
ECM 解読手段
24
EMM 解読手段
25
ユーザ情報記憶手段
26
認証鍵交換手段
52
D-I/F
51
DMUX
57
MUX
54
記録処理手段
55
再生処理手段
58
D
Kco
Kco(D)
SERVPa(Kco)
SERVSa
Kw

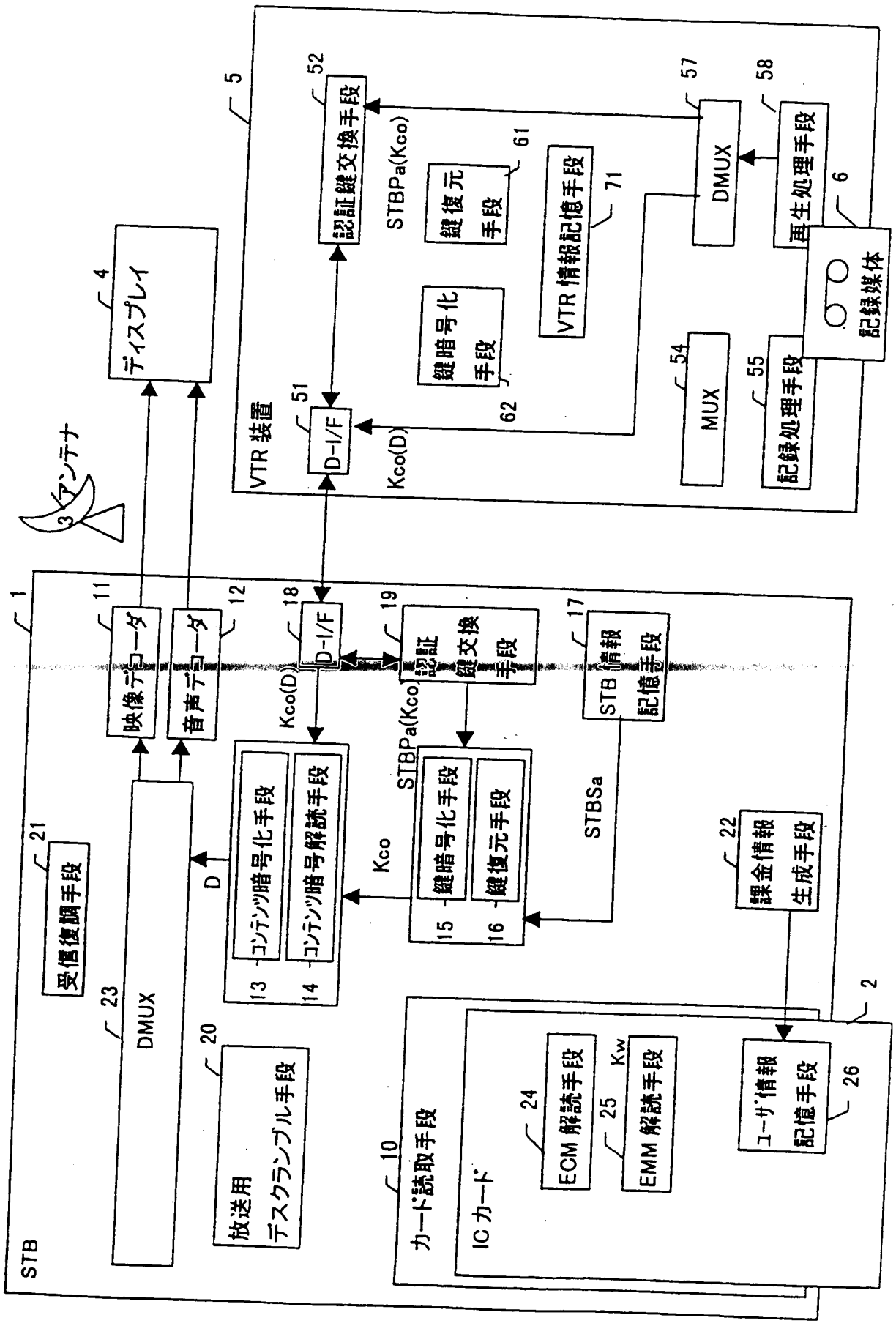
第１０図



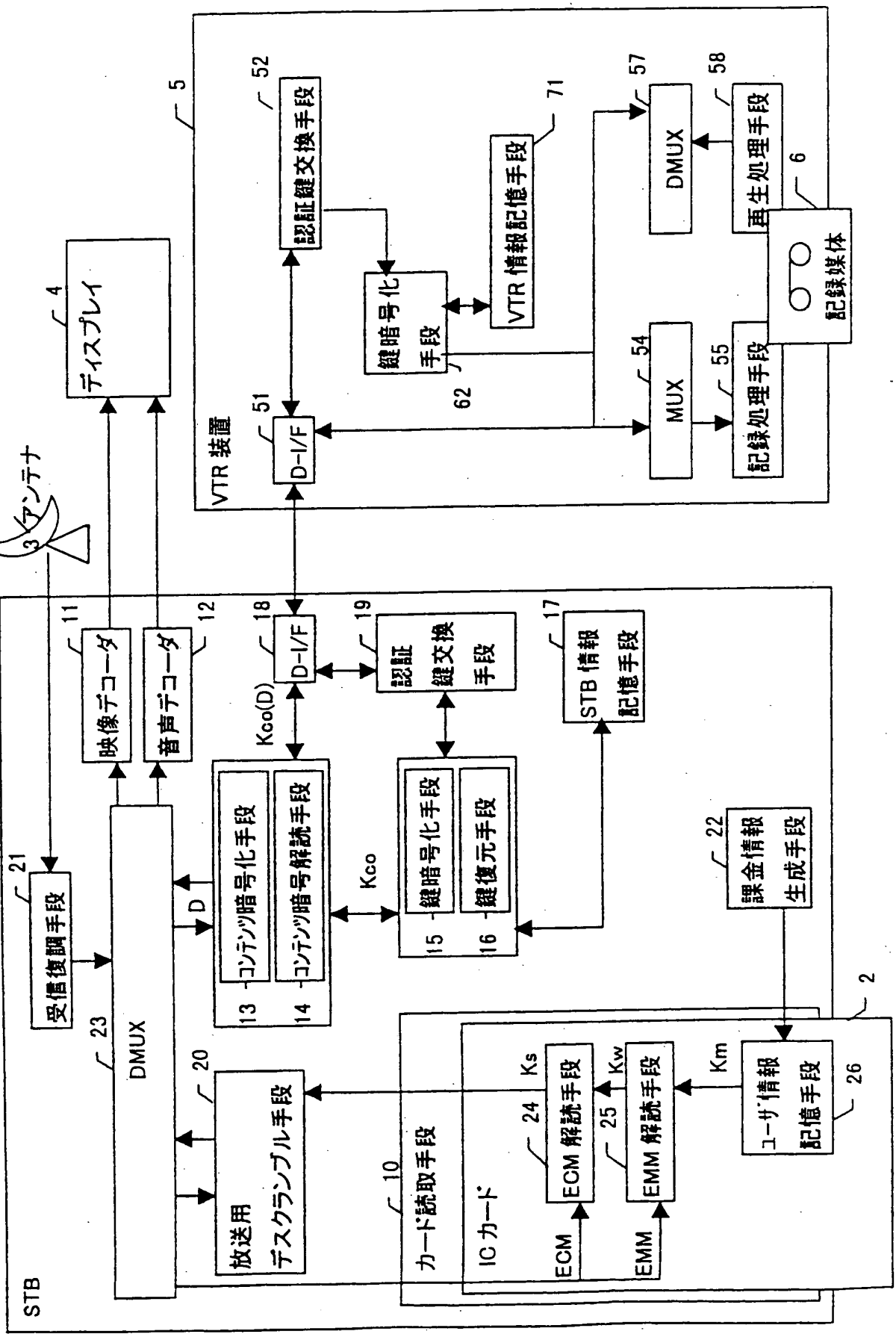
第１１図


STB
1
アンテナ
3
ディスプレイ
4
VTR 装置
5
再生処理手段
6
記録媒体
DMUX
57
58
認証鍵交換手段
52
鍵復元手段
61
鍵暗号化手段
62
VTR 情報記憶手段
71
D-I/F
51
MUX
54
記録処理手段
55
Kx(Kco)
Kco
Kx
STBPa
STBPa(Kco)
Kco(D)
D-I/F
18
認証鍵交換手段
19
STB 情報記憶手段
17
映像デコーダ
11
音声デコーダ
12
コンテンツ暗号化手段
13
鍵暗号化手段
15
受信復調手段
21
DMUX
23
課金情報生成手段
22
放送用デスクランブル手段
20
カード読取手段
10
IC カード
ECM 解読手段
24
EMM 解読手段
25
ユーザ情報記憶手段
26
Ks
Kw
Km
ECM
EMM
D
2

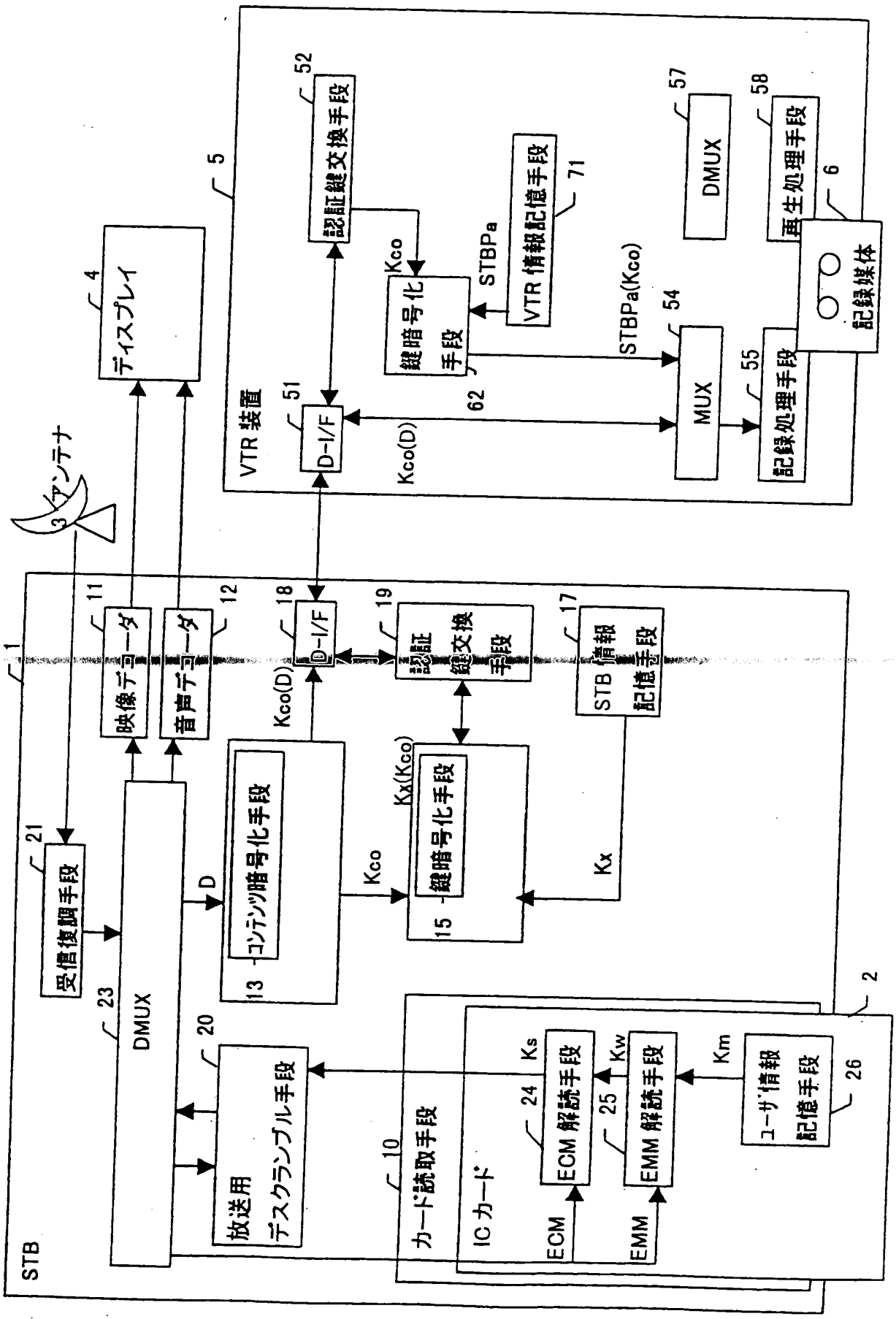
第１２図



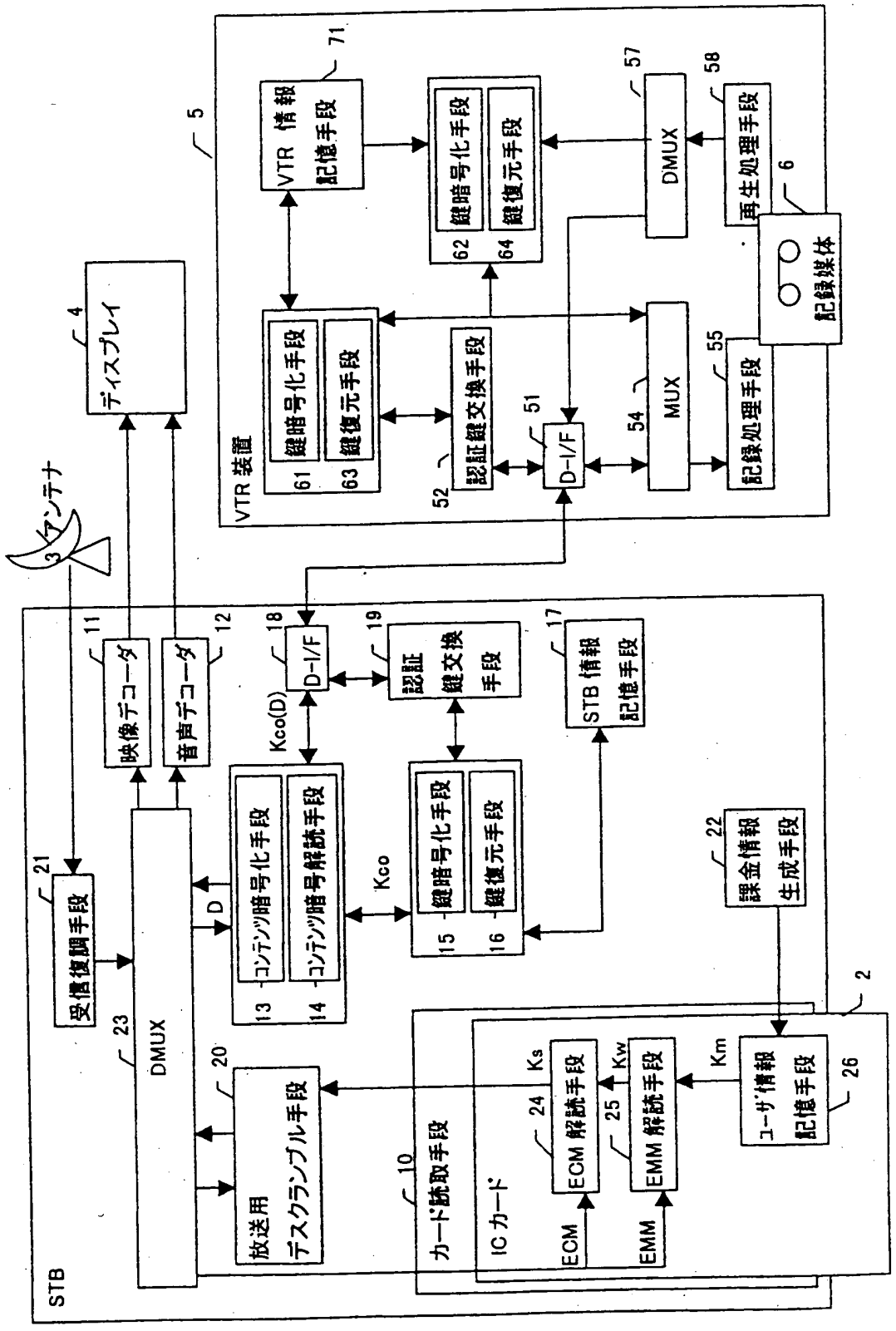
第１３図



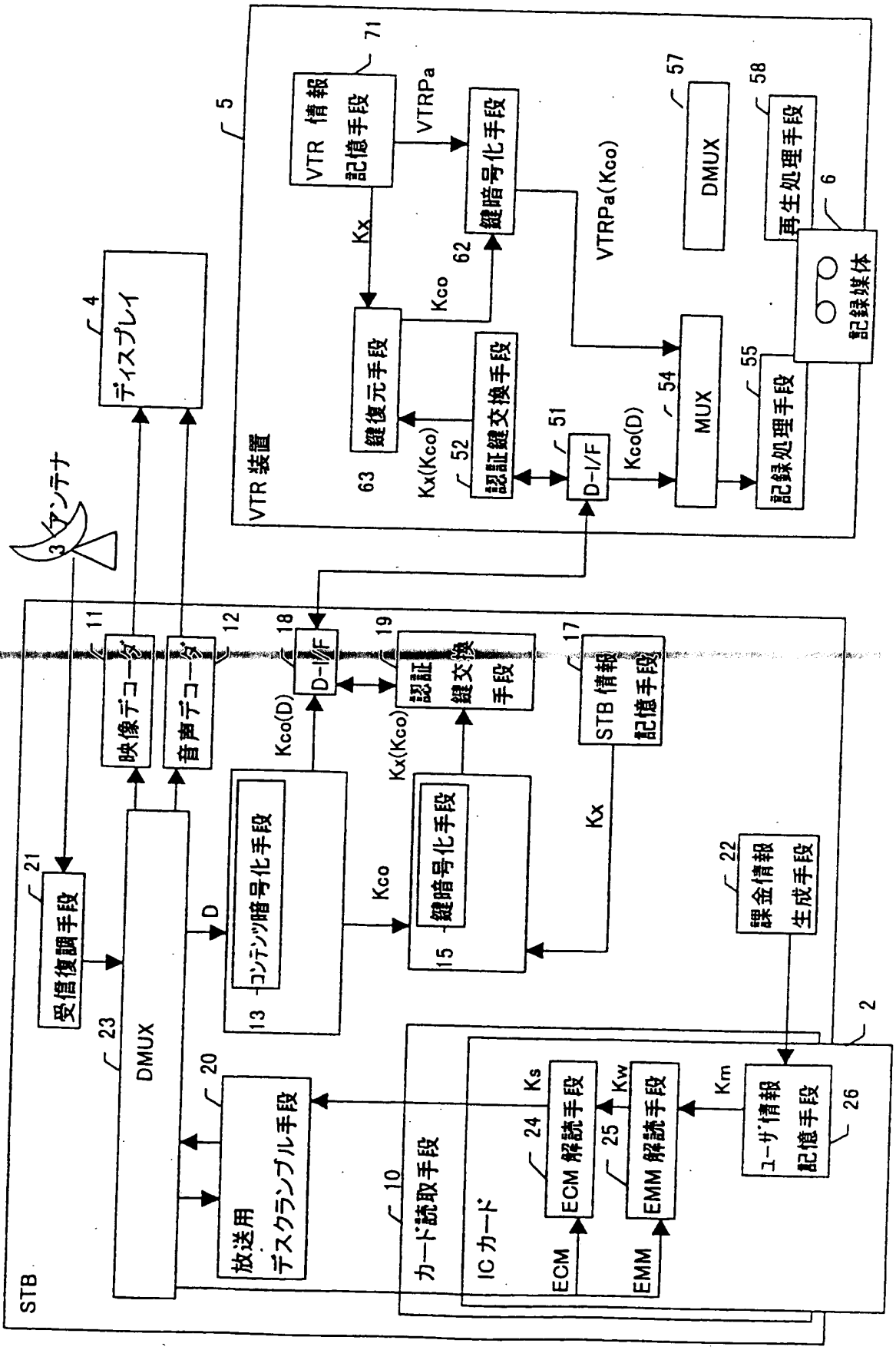
第１４図



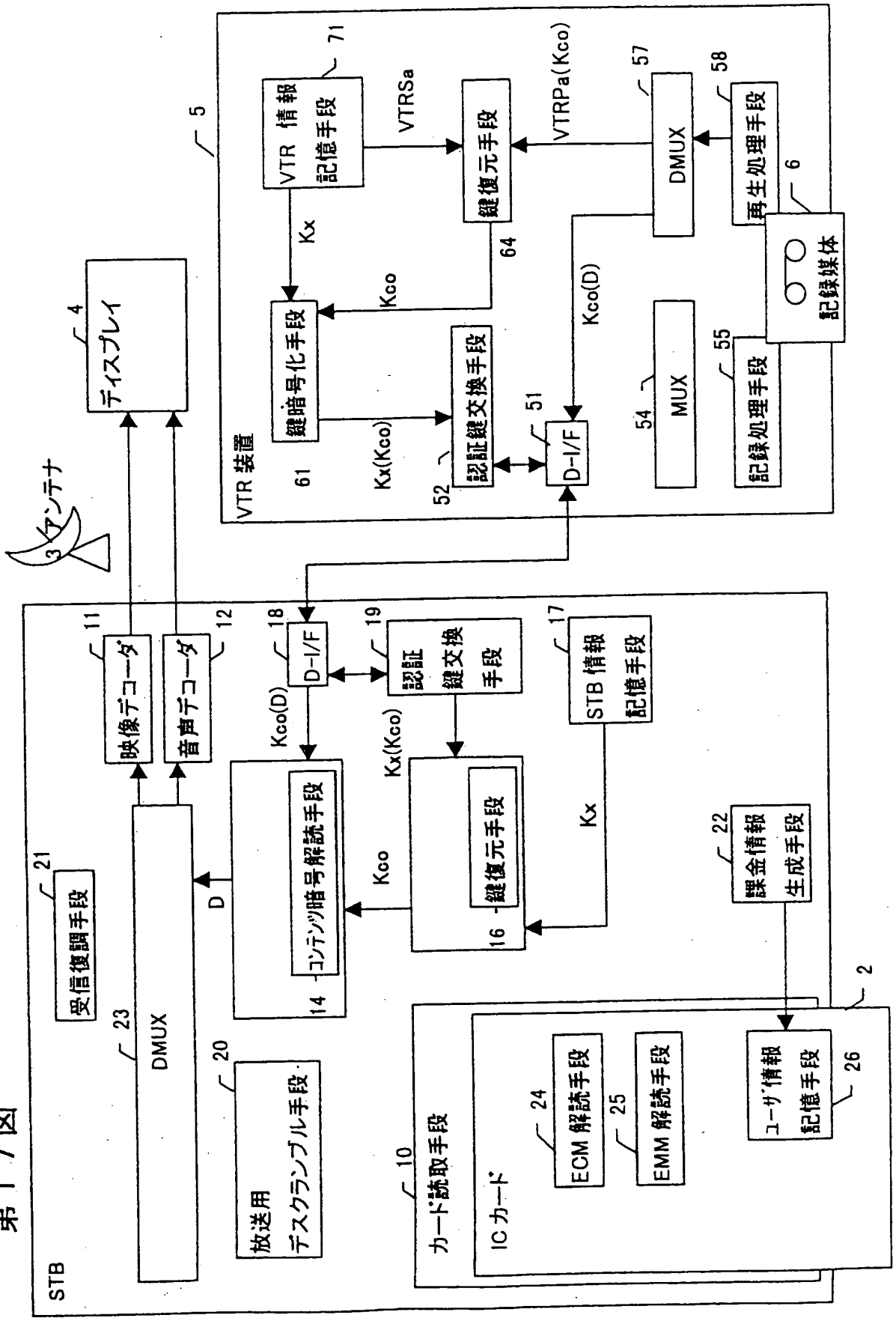
第１５図


STB
VTR 装置
ディスプレイ
アンテナ
映像デコーダ
音声デコーダ
受信復調手段
DMUX
放送用 デスクランブル手段
コンテンツ暗号化手段
コンテンツ暗号解読手段
D-I/F
認証 鍵交換 手段
鍵暗号化手段
鍵復元手段
STB 情報 記憶手段
課金情報 生成手段
カード識取手段
IC カード
ECM 解読手段
EMM 解読手段
ユーザ情報 記憶手段
VTR 情報 記憶手段
認証鍵交換手段
MUX
記録処理手段
再生処理手段
記録媒体
Kco(D)
Kco
Ks
Kw
Km
ECM
EMM

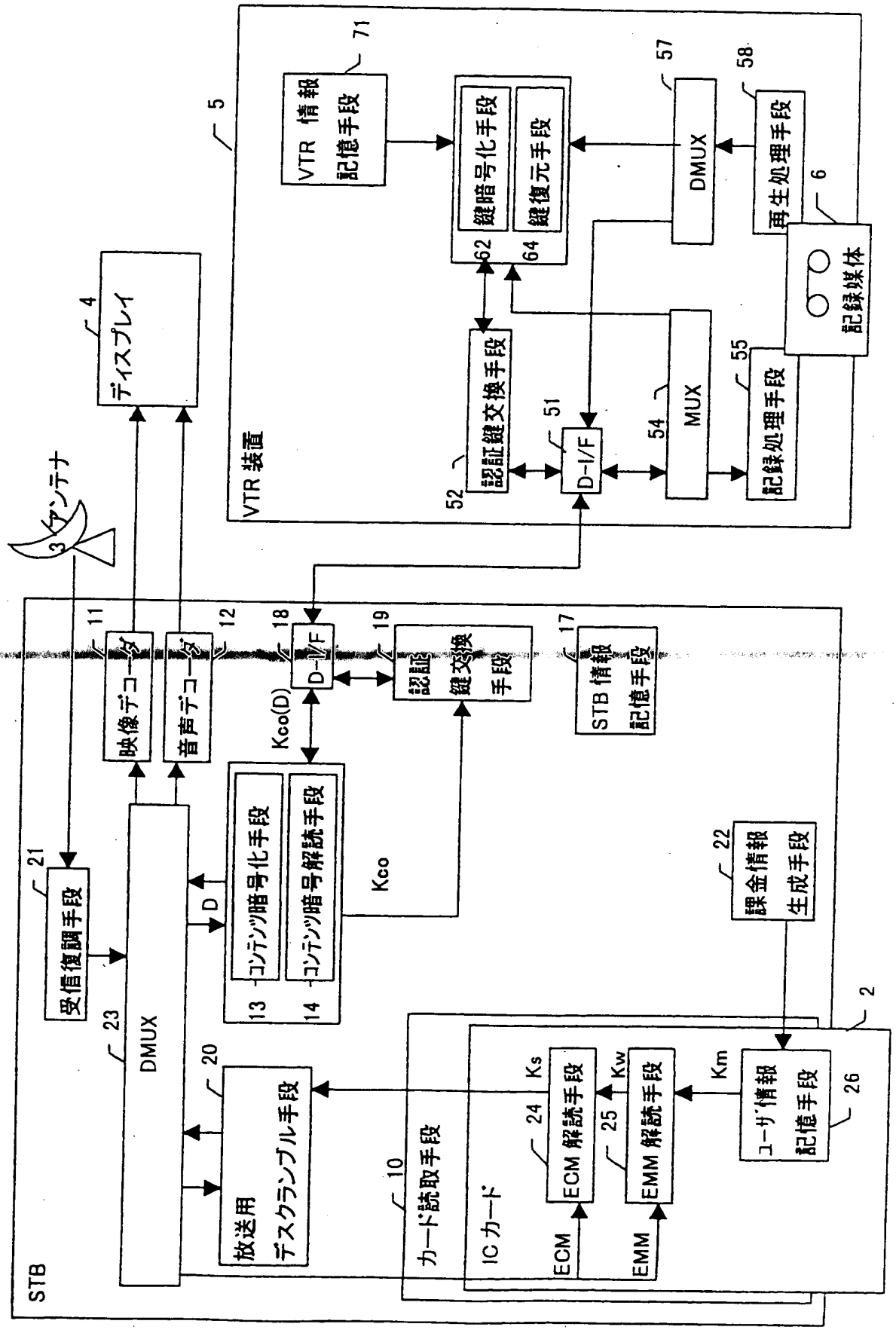
第16図



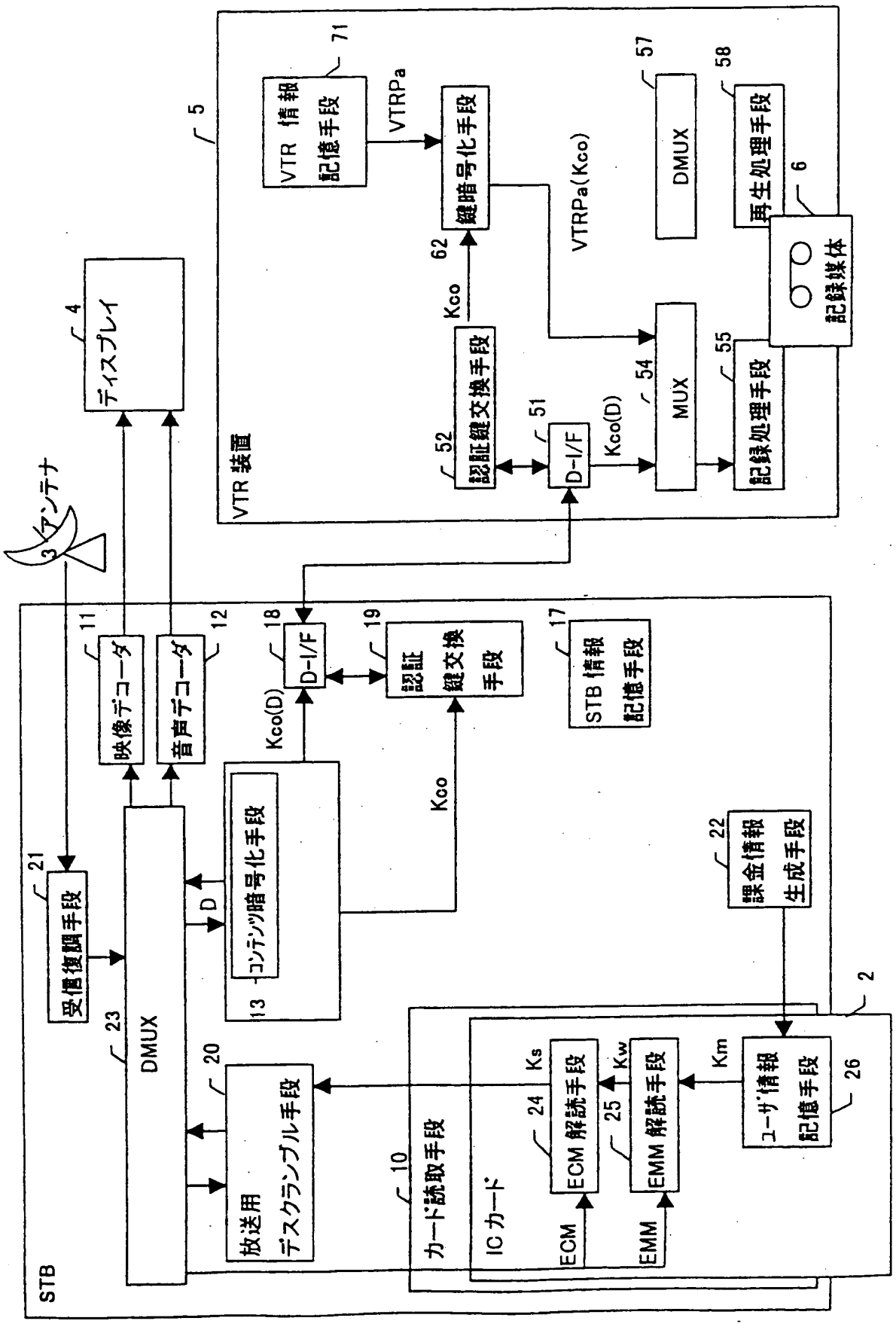
第１７図


STB
VTR 装置
5
VTR 情報 記憶手段
71
VTRSa
鍵復元手段
VTRPa(Kco)
DMUX
57
再生処理手段
58
6
記録媒体
Kx
64
Kco
鍵暗号化手段
61
Kx(Kco)
認証鍵交換手段
52
D-I/F
51
Kco(D)
MUX
54
記録処理手段
55
4
ディスプレイ
3
アンテナ
11
映像デコーダ
12
音声デコーダ
18
D-I/F
19
認証 鍵交換 手段
17
STB 情報 記憶手段
Kco(D)
Kx(Kco)
コンテンツ暗号解読手段
14
鍵復元手段
16
Kco
Kx
D
21
受信復調手段
23
DMUX
20
放送用 デスクランブル手段
22
課金情報 生成手段
2
カード読取手段
10
IC カード
24
ECM 解読手段
25
EMM 解読手段
ユーザ情報 記憶手段
26

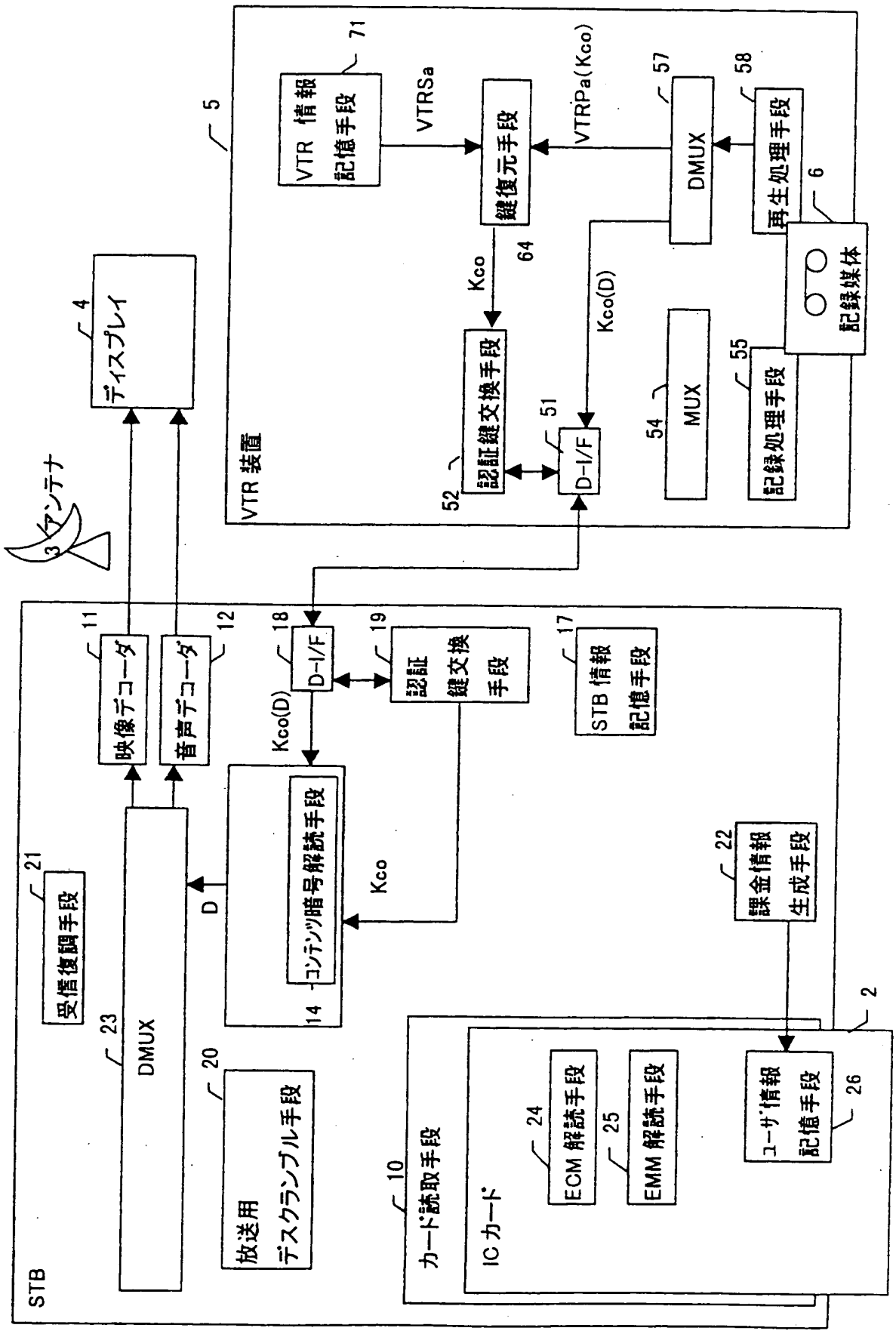
第１８図



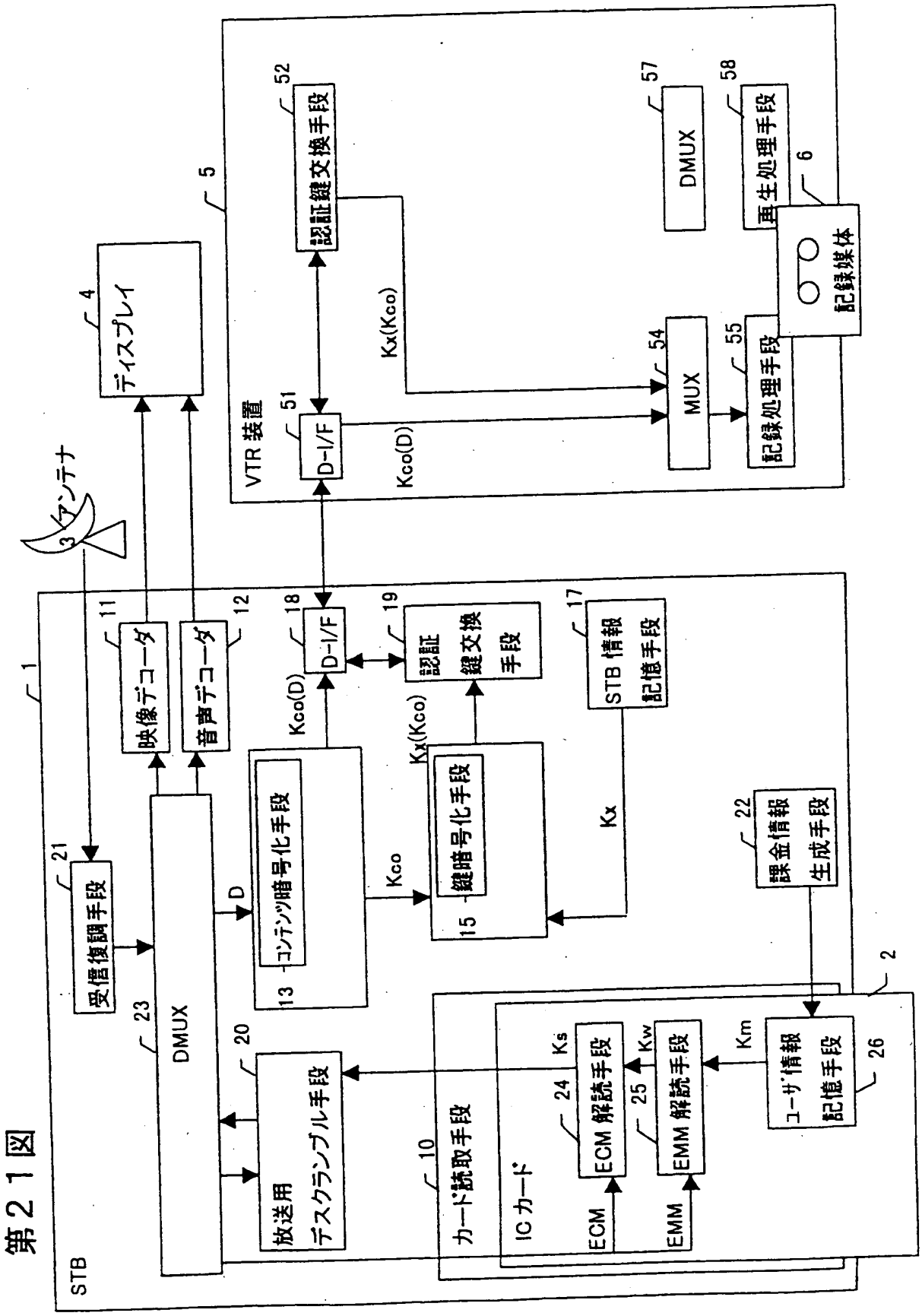
第１９図



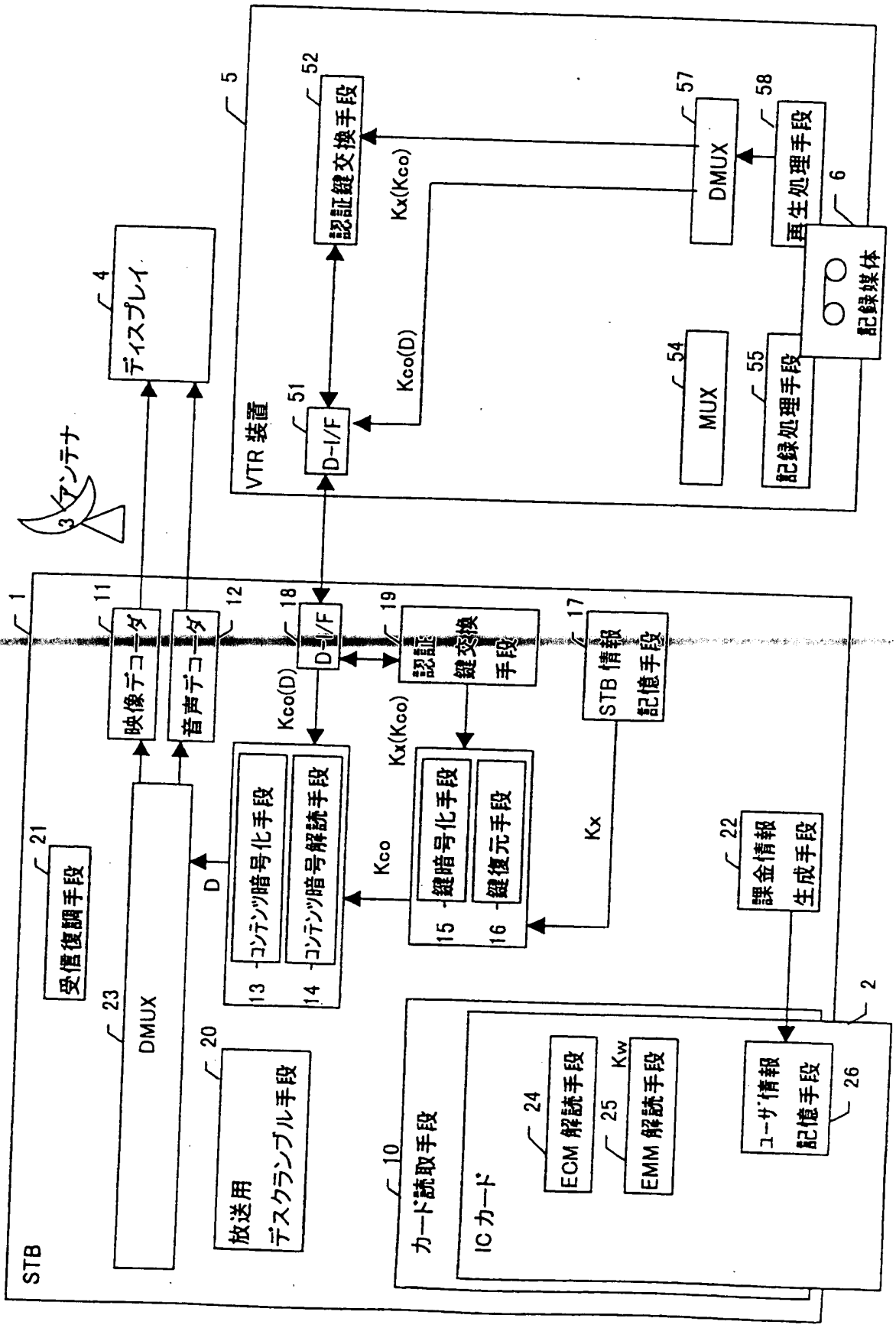
第２０図



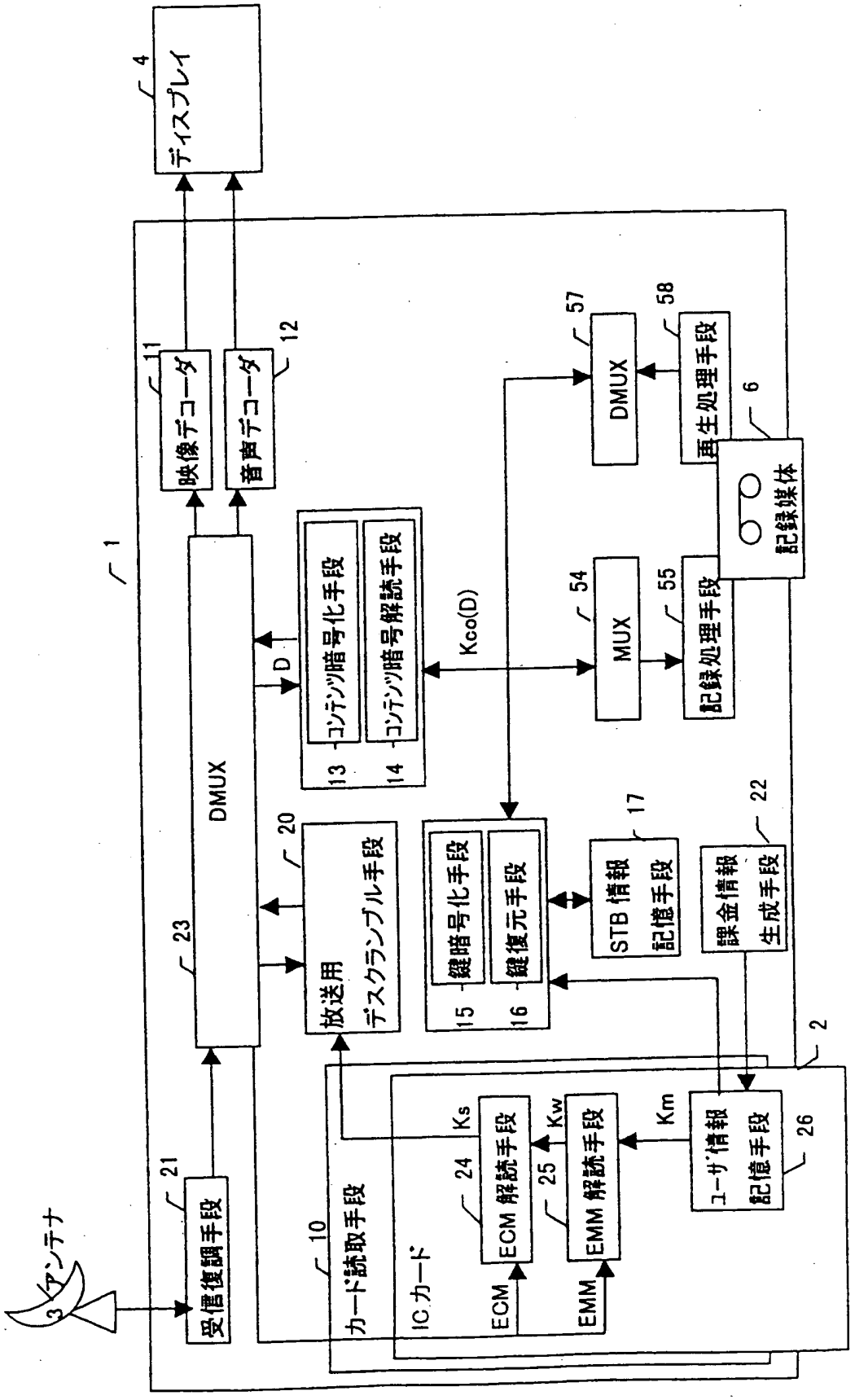
第２１図



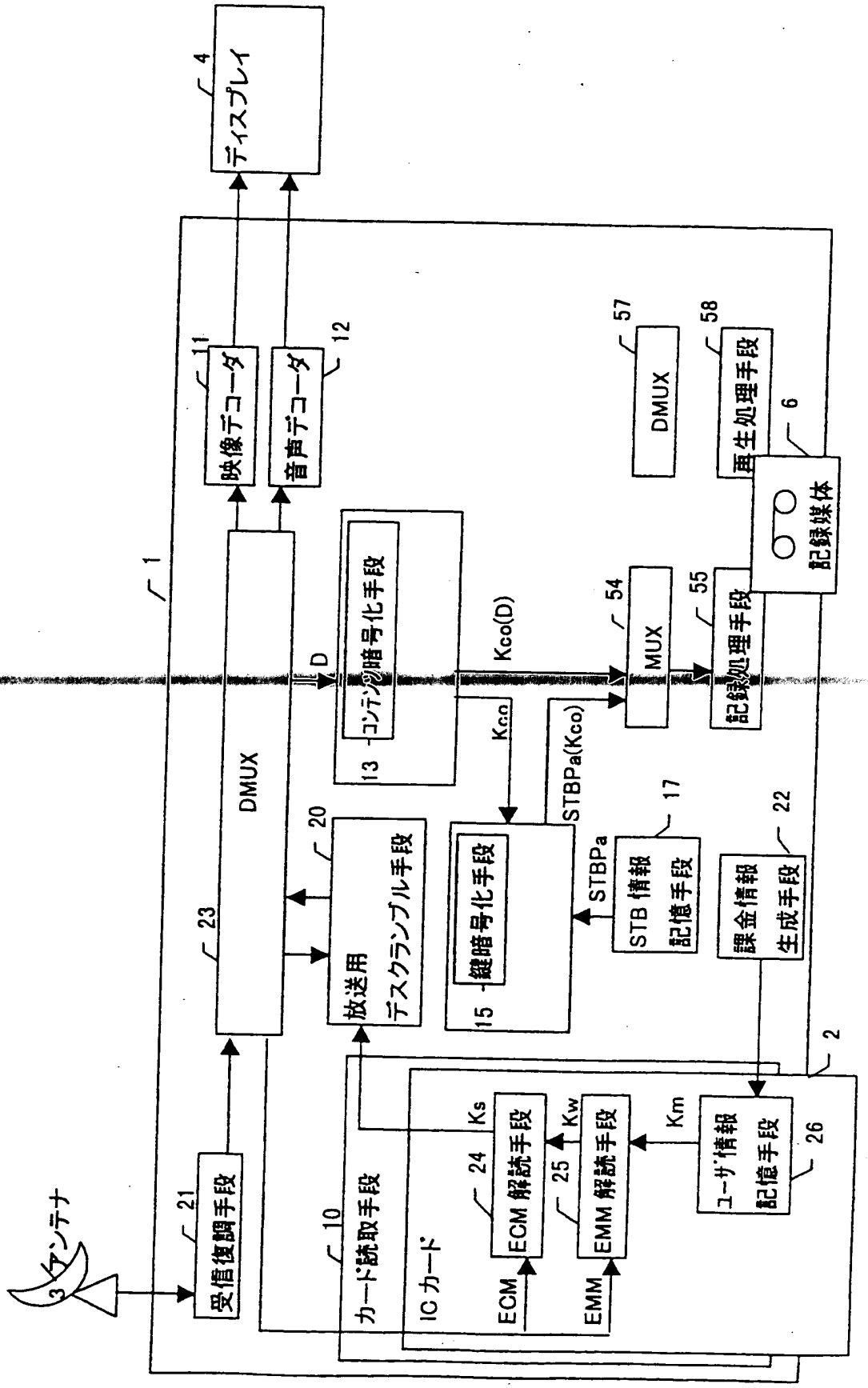
第22図



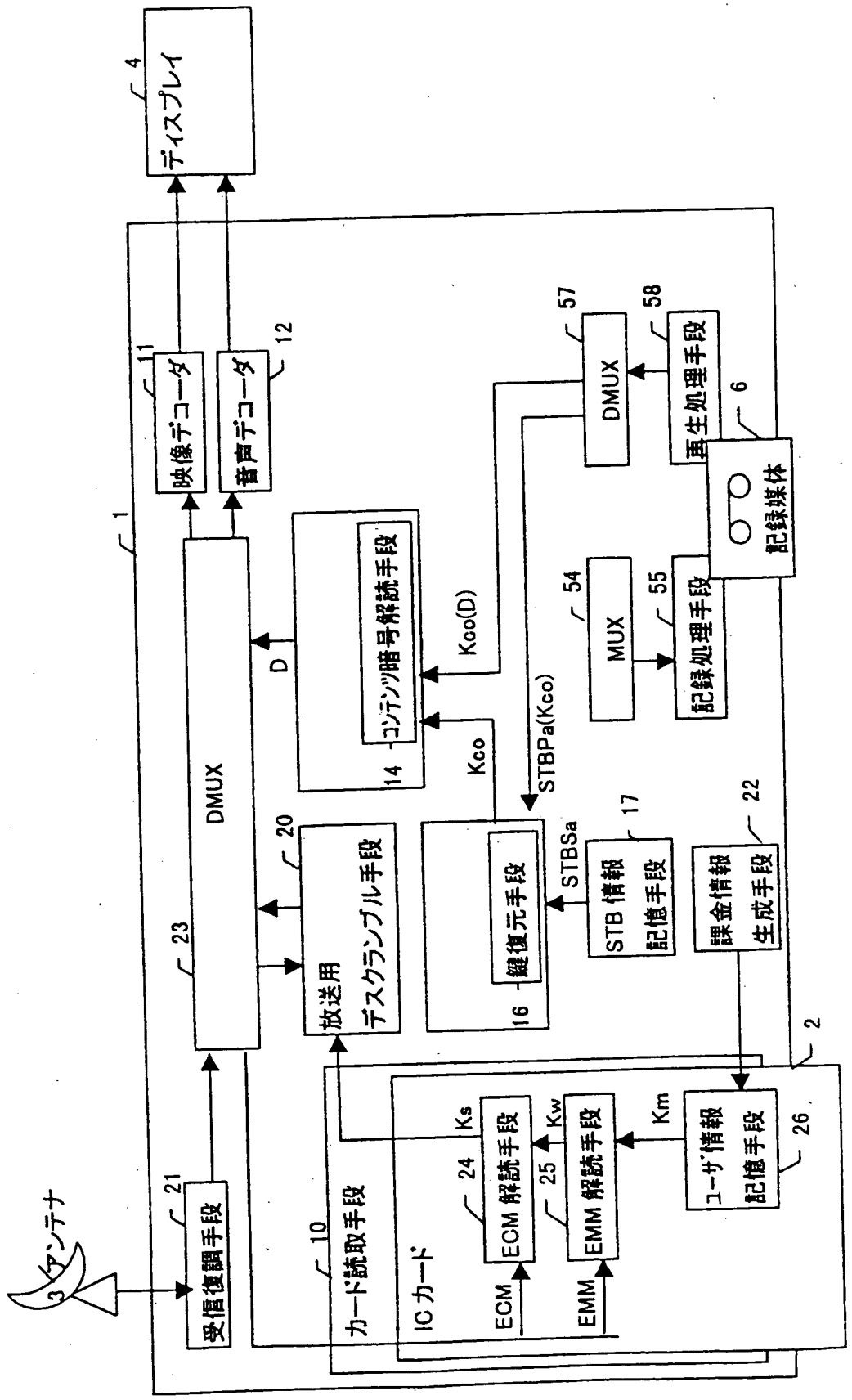
第２３図


アンテナ
3
受信復調手段
21
IC カード
カード読取手段
10
ECM
EMM
ECM 解読手段
24
EMM 解読手段
25
Ks
Kw
Km
ユーザ情報記憶手段
26
課金情報生成手段
22
STB 情報記憶手段
17
鍵暗号化手段
15
鍵復元手段
16
放送用デスクランブル手段
20
DMUX
23
コンテンツ暗号化手段
13
コンテンツ暗号解読手段
14
D
Kco(D)
MUX
54
記録処理手段
55
DMUX
57
再生処理手段
58
記録媒体
6
映像デコーダ
11
音声デコーダ
12
ディスプレイ
4
1
2

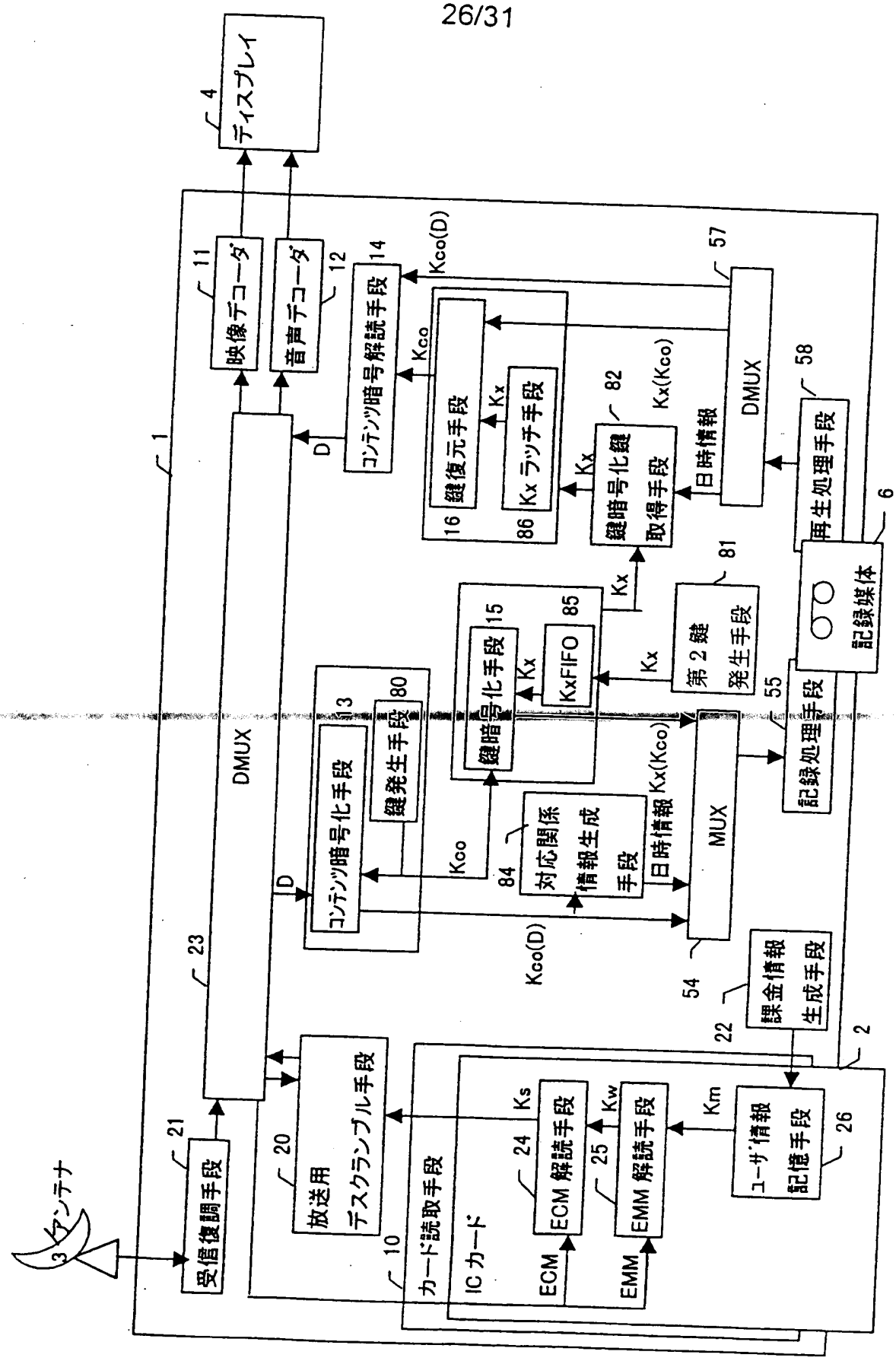
第２４図



第２５図


ディスプレイ
4
映像デコーダ
11
音声デコーダ
12
1
DMUX
23
D
コンテンツ暗号解読手段
14
Kco(D)
Kco
STBPa(Kco)
DMUX
57
再生処理手段
58
6
記録媒体
MUX
54
記録処理手段
55
放送用
デスクランブル手段
20
鍵復元手段
16
STBSa
STB情報
記憶手段
17
課金情報
生成手段
22
2
ICカード
カード読取手段
10
ECM解読手段
24
EMM解読手段
25
ユーザ情報
記憶手段
26
Ks
Kw
Km
ECM
EMM
受信復調手段
21
アンテナ
3

第２６図



第２７図

暗号化鍵 Kx リスト

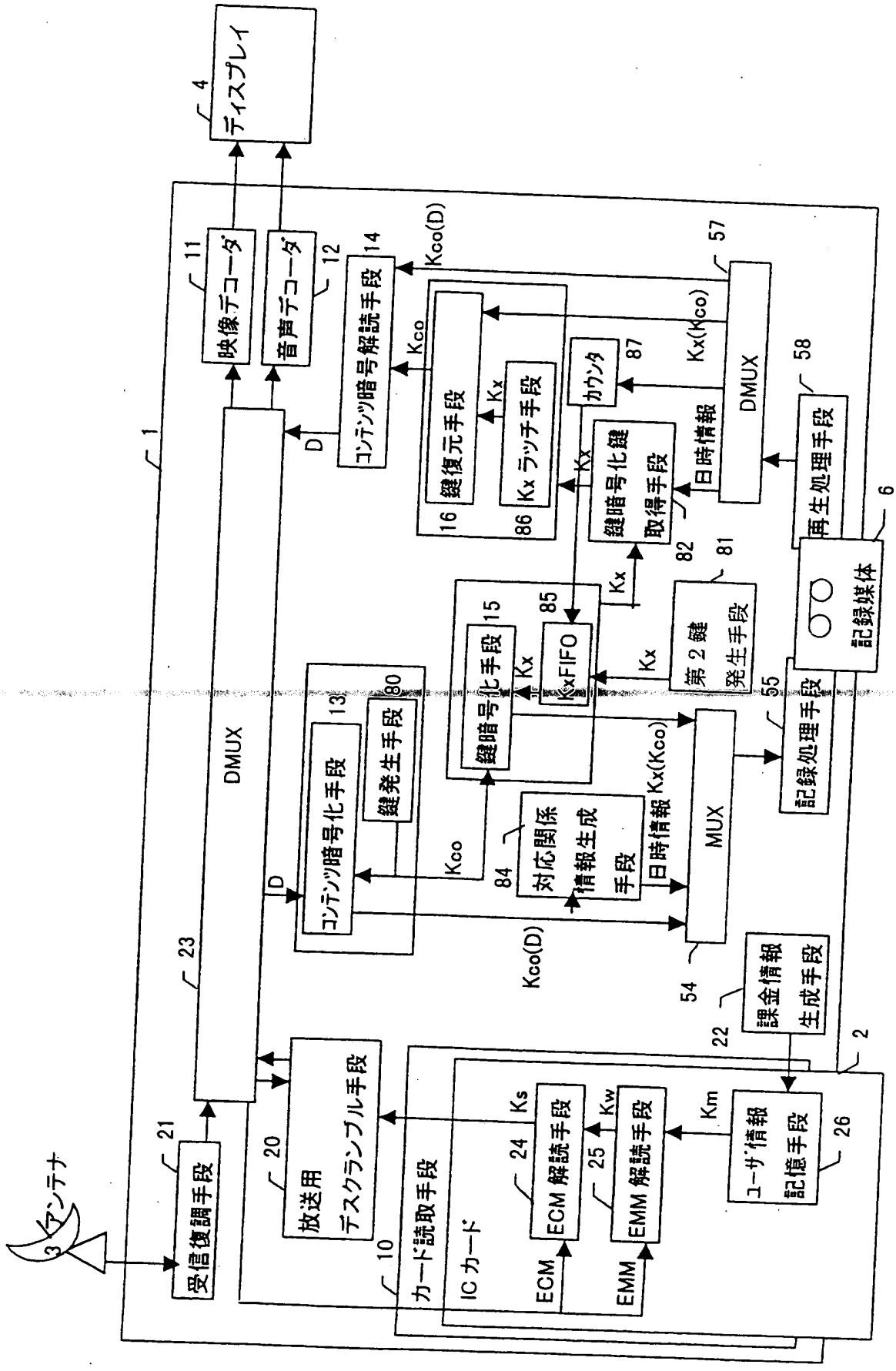
(a) １月4日現在

No.	暗号化鍵	鍵発生日
1	Kc4	１月４日
2	Kc3	１月３日
3	Kc2	１月２日
4	Kc1	１月１日
5		
6		
7		

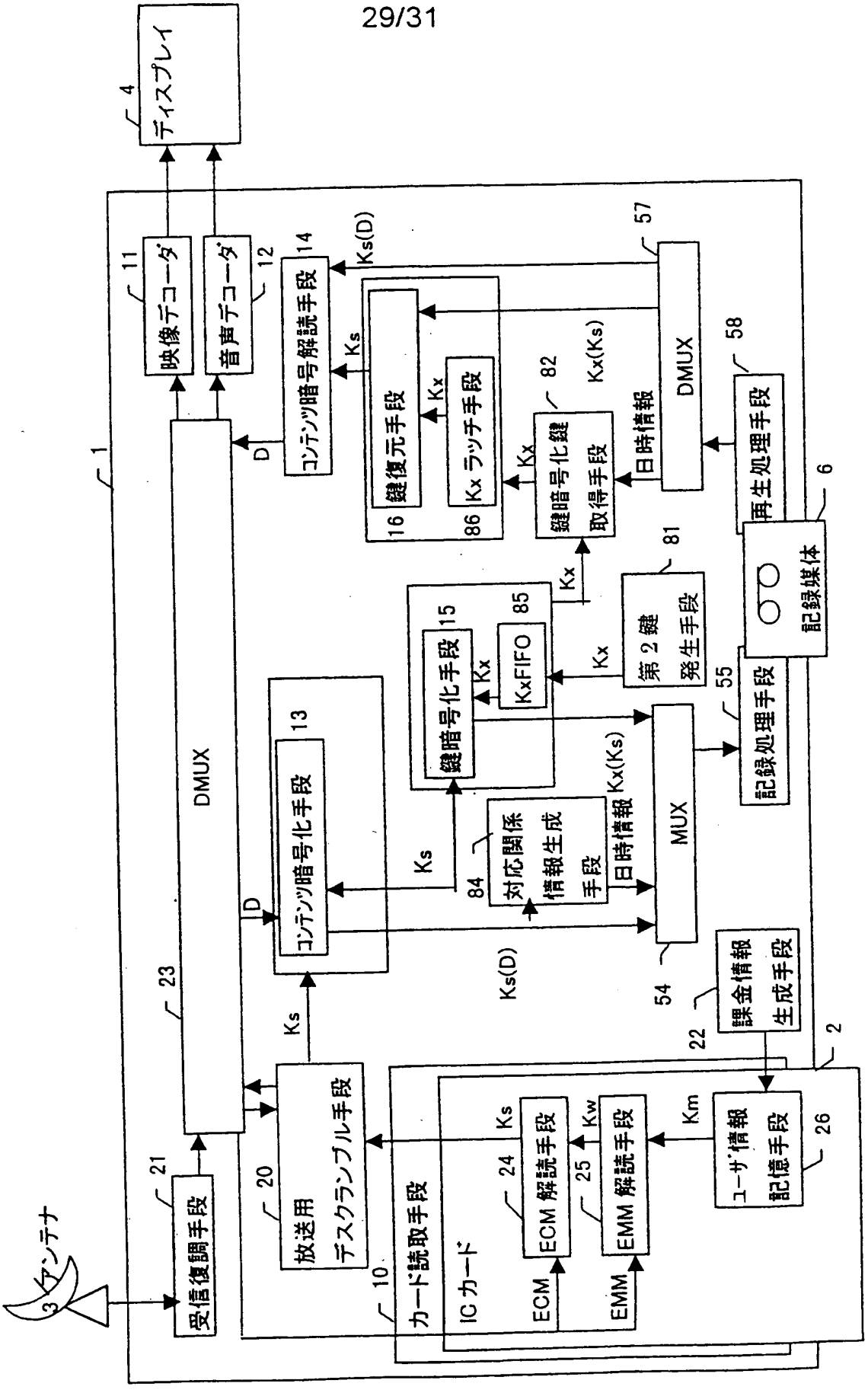
(b) １月９日現在

No.	暗号化鍵	鍵発生日
1	Kc9	１月９日
2	Kc8	１月８日
3	Kc7	１月７日
4	Kc6	１月６日
5	Kc5	１月５日
6	Kc4	１月４日
7	Kc3	１月３日

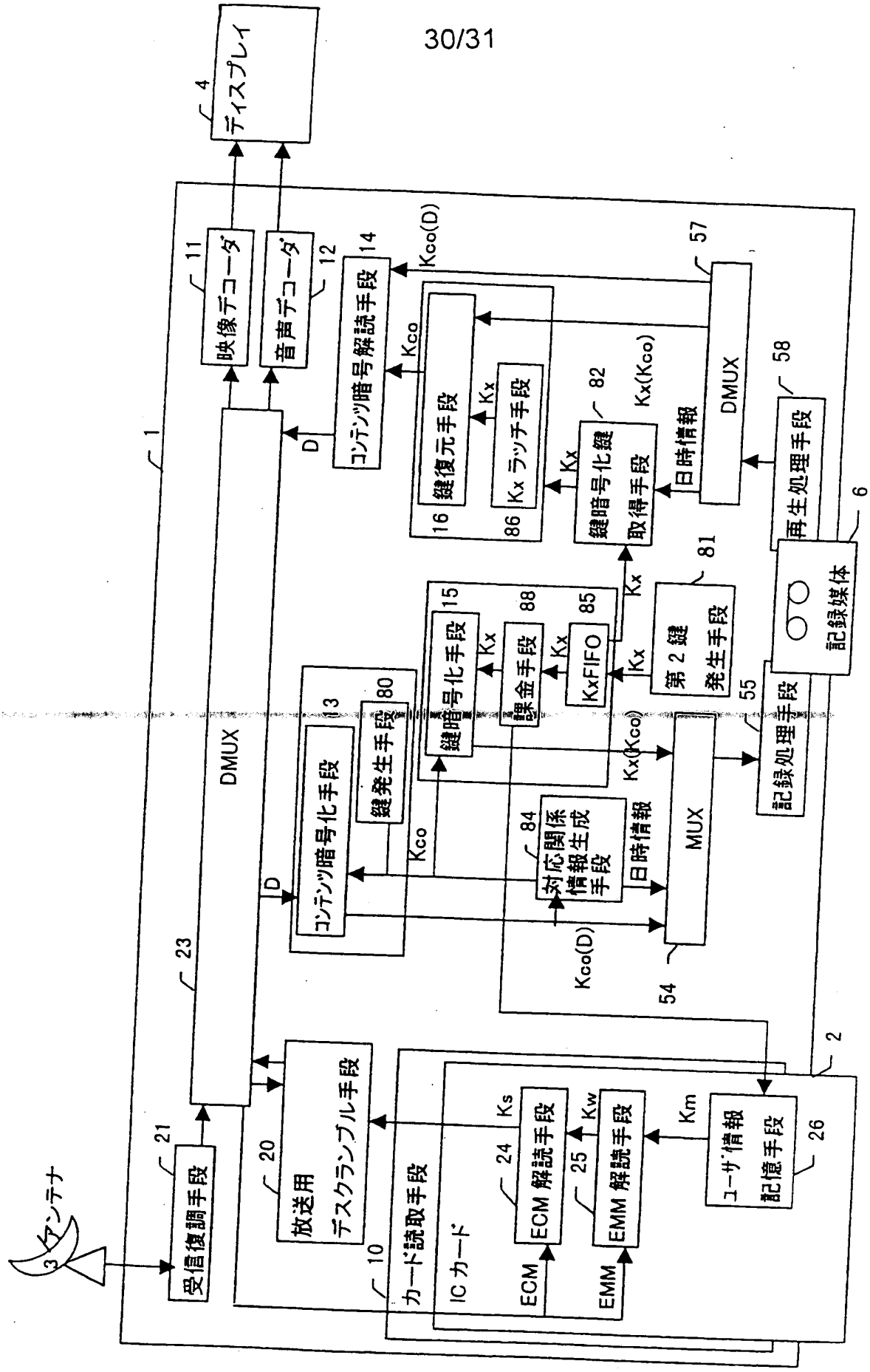
第２８図



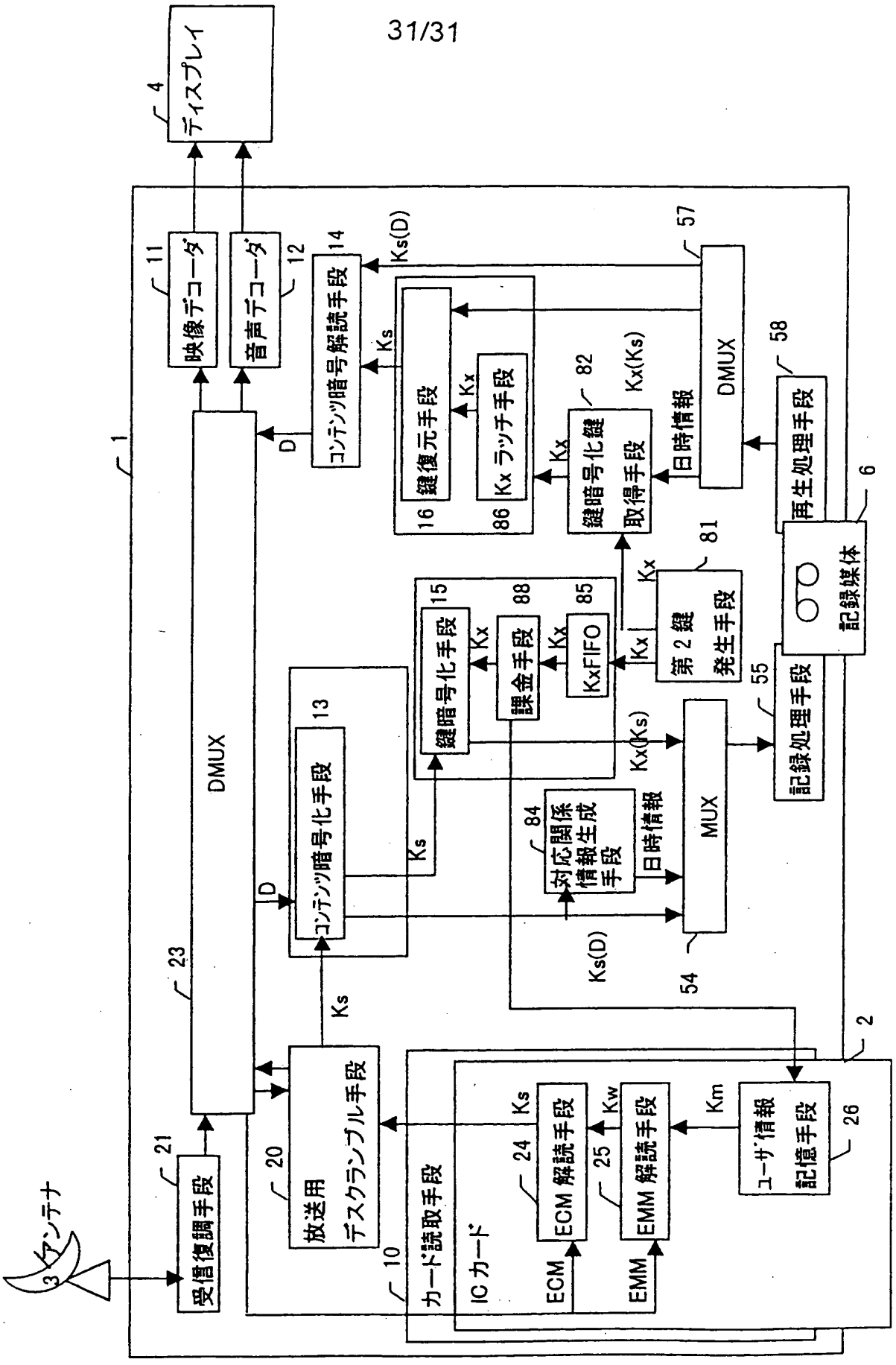
第２９図



第３０図



第３１図



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/00292

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] G11B20/10, H04N5/91

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] G11B20/10, H04N5/91

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP, 7-272399, A (Hitachi,Ltd.), 20 October, 1995 (20. 10. 95), Full text ; Figs. 1 to 18 Full text ; Figs. 1 to 18 Full text ; Figs. 1 to 18 (Family: none)	1, 4, 6 2, 3, 5 7-66
A	JP, 7-288798, A (Mitsubishi Electric Corp.), 31 October, 1995 (31. 10. 95), Full text ; Figs. 1 to 10 (Family: none)	11-14, 21
A	JP, 9-214929, A (Toshiba Corp.), 15 August, 1997 (15. 08. 97), Full text ; Figs. 1 to 6 (Family: none)	22-28
A	JP, 8-77706, A (Sony Corp.), 22 March, 1996 (22. 03. 96), Full text ; Figs. 1 to 7 (Family: none)	39-62

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 April, 1999 (19. 04. 99)	27 April, 1999 (27. 04. 99)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　PCT／JP99／00292

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl[6]　G11B20／10, H04N5／91

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl[6]　G11B20／10, H04N5／91

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－1999年
日本国登録実用新案公報　1994－1999年
日本国実用新案登録公報　1996－1999年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
	JP, 7－272399, A（株式会社日立製作所）20. 10月. 1995（20. 10. 95）	
X	全文，第1－18図	1，4，6
Y	全文，第1－18図	2，3，5
A	全文，第1－18図（ファミリーなし）	7－66
A	JP, 7－288798, A（三菱電機株式会社）31. 10月. 1995（31. 10. 95）全文，第1－10図（ファミリーなし）	11－14，21
A	JP, 9－214929, A（株式会社東芝）15. 8月. 1997（15. 08. 97）全文，第1－6図（ファミリーなし）	22－28

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
19. 04. 99	27.04.99

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	小松　正　印　5Q　7736 電話番号　03－3581－1101　内線　6922

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９９／００２９２

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ，８－７７７０６，Ａ（ソニー株式会社）２２．３月．１９９６（２２．０３．９６） 全文，第１－７図（ファミリーなし）	３９－６２

様式ＰＣＴ／ＩＳＡ／２１０（第２ページの続き）（１９９８年７月）